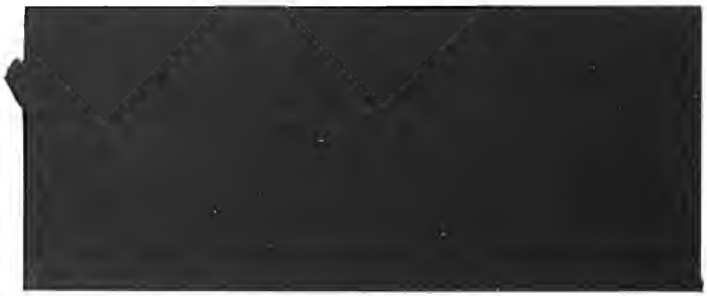
PRIVACY AND THE AMERICAN CITIZEN

Peter Bloomsburgh
Edouard M. Cointreau
Richard C. Owens
Stephen J. Williams

February 1971

559-71
September



PRIVACY AND THE AMERICAN CITIZEN

Peter Bloomsburgh
Edouard M. Cointreau
Richard C. Owens
Stephen J. Williams

February 1971 559-71
September

PRIVACY AND THE AMERICAN CITIZEN

February 1971

Massachusetts Institute of Technology
Alfred P. Sloan School of Management
50 Memorial Drive
Cambridge, Massachusetts, 02139

In order to successfully apply the techniques and theories of management to real-world decision making, it is necessary to understand the context in which those decisions are made.

In this vein, Dr. Richard S. Morse, of the Sloan School of Management at M.I.T., has offered the course "The Government/Industry Environment." The purpose of the course is two-fold: to provide an understanding of public policy-making, and to investigate a specific current problem involving the public sector.

The work reported here is a result of that course. The content and conclusions are those of the authors, and do not necessarily represent the views of either Dr. Morse or the Sloan School.

Richard S. Morse
Cambridge, Massachusetts
February 1971

"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.... The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process...in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms."

--Alan F. Westin

ACKNOWLEDGEMENTS

The assistance of many individuals was required in the preparation of this report.

Dr. Richard Morse and Mr. Eric Rule, of the Alfred P. Sloan School of Management at M.I.T., provided invaluable advice and support.

Dr. Robert M. Fano, of Project MAC at M.I.T., provided insight into the general issues as well as much technical advice.

General Harold K. Johnson, U. S. Army (ret.), Colonel John Downie, and Mr. Ronald Greene, of the Department of the Army, Mr. Christopher Pyle, of Columbia University, Dr. Herbert Holliman, of M.I.T., and Dr. Paul Weaver of Harvard all submitted graciously to our interviewing.

Mrs. Marjorie Swindell of the Sloan School at M.I.T. provided generous administrative assistance.

TABLE OF CONTENTS

PART I: SUMMARY OF FINDINGS AND CONCLUSIONS

One of the major problems of American society today is the lack of a widely accepted definition of privacy. At least one excellent definition exists, as presented by Alan Westin, and it highlights the constant tradeoff which must be made between the individual's desire to be an individual, and his desire to be a member of society. In order to preserve its norms, society sets certain constraints on the individual's privacy decision, and establishes institutions to enforce those constraints. The legal and Constitutional bases for privacy in America are somewhat vague, with the result that some institutions have tended to go beyond the limits of reason in enforcing norms.

The electronic computer, which is an amoral implement for amplifying man's ability to process information, is one tool which some institutions have misused in constraining privacy. Fault in these cases lies not with the computer, but with the institutions themselves. One such institution is the U.S. Army.

The collection of information is not, however, evil; in fact, information collection is a prerequisite to civilization. Given the three basic reasons for collection of data, coupled with a list of criteria for the evaluation of individual data banks, it is reasonably straightforward to evaluate existing or proposed data banks. Such evaluation has historically not been undertaken.

What is needed is a comprehensive national policy for such evaluations, firmly based in analysis of social costs vs. social benefits, and coupled with an effective method of enforcement. Most important of all, however, is the realization by each American that the protection of privacy is a job for him.

PART II: PRIVACY: A FRAMEWORK

A. Justification for Concern

Traditional lack of concern; necessity for consideration by both individuals and society as a whole; current state of thought on the subject.

JUSTIFICATION FOR CONCERN

As a nation, we have traditionally failed to carefully consider questions of fundamental societal values until those values were threatened by the onslought of technological, economic, or sociological developments. And so it is with the basic rights of privacy in our democracy. As the development of technological resources, exemplified by but not limited to the high speed digital computer, continues at an increasingly rapid pace, our abilities to impinge on personal privacy are amplified immensely. The combination of an expanding population, a complex economy, and the increasing availability of electronic equipment of varying capabilities underscores the urgency for the formulation of national policies regarding the wide range of questions related to privacy. We can wait no longer. According to Dr. Allen Westin, Professor of Public Law at Columbia University and a prominent leader in the fight to make privacy a national concern:

> "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."
> (Westin, A., Privacy and Freedom, Ch. 1)

Privacy is a question for everyone to think about; it is not to be left solely to the specialists. Indeed, every time someone completes an application for employment, applies for a driver's license, or applies for a credit card, he is making a decision related to his privacy. Yet although most Americans would agree that no one should take a challenge

to his privacy lightly, few thoughtfully weigh the consequences and implications of applying for a credit card or answering an investigator's questions about their neighbors. We should remember that anytime a transfer of information occurs, privacy is in some way impinged, whether it be our personal privacy, that of our friends and neighbors, or the privacy of some other individual or organization.

Concurrently with our individual consideration of questions of privacy, we must act as a nation to forge a clear national policy.

The media have consistently demonstrated an awareness that questions of privacy must be explored. According to the New York Times (Aug. 9, 1966), in an editorial regarding the 1966 proposal for a National Data Bank for collecting all government files in a central depository:

> "Can personal privacy survive the ceaseless advances of the technological juggernaut?...Aside from the opportunities for blackmail and from the likelihood that the record of any single past transgression might damage one for life, this proposed device would approach the effective end of privacy...."

The recent emphasis on the necessity of law and order coupled with calls from many sectors of the population for a crackdown on crime and violence has served to emphasize the urgency of developing a national policy with respect to privacy, particularly as related to federal, state, and local governments. A recent editorial in the Wall Street Journal by David C. Anderson (Nov. 4, 1970) discussed this problem:

"...Other new technologies grew to have an even more direct relevance to the increased threat to democratic freedoms.

"Recent advances in electronic miniaturization and other areas vastly increased the range and efficiency of eavesdropping devices for example.

"And the uncomfortable implications of such increased capability were hardly diminished by the desire of some public officials sto claim broad powers to use it. Attorney General John Mitchell felt free to declare unilaterally and rather formally last year...that Government agents had a right to eavesdrop on anybody the Attorney General decides is a threat to the national security, without any court review, and without having to disclose what has been overheard.

"Computers have also had an impact...it was disclosed that various agencies of Government had created a computerized data bank to centralize the information the Government collects on citizens and make it available at the punch of a key."

The rhetoric of concern has not been confined to the media, however. The halls of Congress, from whence any national legislative limitations on the invasion of privacy must emerge, have echoed with considerable concern on the parts of our elected representatives.

Hearings by the Administrative Practice and Procedure Subcommittee of the Senate held in 1965 revealed such practices as maintaining peepholes in ladies' locker rooms and rest rooms in post offices throughout the country. During the same hearings, the committee discovered that Internal Revenue Service agents had utilized mail covers, and had in some cases opened first-class mail. Other controversial practices were also discovered. These hearings lead Senator Edward Long, Chairman of the subcommittee, to conclude that:

> "This investigation has been but one small battle in the campaign against Big Brother, but it is my earnest hope that it has demonstrated that the only way to beat him is by constant exposure of his bully boys and agents, and by forcing him to realize that, like the rest of us, they are going to be held responsible for their actions." (Long, E., Playboy, n.d.)

U. S. Congressman Cornelius Gallagher, speaking to the Ninth Practicum on Practical Politics (Jersey City, State College, May 7, 1968), discussed some conclusions he had drawn from the hearings on the National Data Bank proposal:

> "...it is my opinion that the most important domestic problem facing our Nation today is re-establishing the stability of our urban oriented culture. New methods of data manipulation are necessary to deal with our expanding and highly mobile population, but the efficiency of computerized general categories may be programming out of our society the awareness of those personal differences which define humanity."

Addressing a symposium conducted by ?Computer Audit Systems, Congressman Frank Horton, a member of the Special Subcommittee on Invasion of Privacy of the Committee on Government Operations, also discussed the problems of government data banks:

> "Our concern then, and our concern now, is that a massive compilation of citizen records would present an unacceptable threat to the continuation of individual privacy and democratic safeguards." (

Senator Sam Ervin, a leading proponent of strict controls against invasions of privacy, considers the problem of sufficient magnitude to warrant a federal agency devoted exclusively to protection against technological invasion of privacy. Speaking to the Senate

on November 10, 1969, he stated:

> "Millions of private citizens face...surveillance by computers in private industry as well as in Government. Their problems are equally deserving of attention.
>
> "Due to the national dimensions of this problem and its complicated nature, it is well neigh impossible for Congress, by any one law, to control the dangers posed to our society by computer technology.
>
> "For this reason, in addition to bills prohibiting the collection and use of federal data on individuals, there is an immediate need for establishment of an independent regulatory agency to control this new communication-surveillance system."
> (Congressional Record, vol 115/no. 184)

The executive branch of the federal government has also expressed concern for the problems of privacy, although tangible guidelines for protecting citizens from invasions of privacy have not been promulgated to any significant extent. Recognition of the existence of the problem can be documented, although constructive and definite action appears to be lacking. According to Senator Ervin, in his comments announcing the publication of hearings on privacy and the census:

> "The President has thus far offered no constructive solutions to the constitutional rights issues raised in these hearings. The Administration has taken the easy way out. It has appointed a Presidential Commission to study the problem of government statistical questionnaires. So far we have heard nothing from it.... Another commission, appointed over a year ago by Secretary of Commerce Stans, has also not been heard from so far."
> (Press release of the Senate Subcommittee on Constitutional Rights)

In a letter to Senator Ervin, the Secretary of Health, Education, and Welfare -- Elliot Richardson -- expressed his department's concern over privacy:

> "Social Security numbers are currently being used throughout industry and government as a means of clearly identifying individuals and avoiding the confusion and mistakes which can arise when a number of individuals have common or similar names.... Only in certain clearly defined and very limited circumstances -- circumstances involving national security, administration of the Internal Revenue Act, and administration of the Social Security program itself -- could they be used in obtaining information from Social Security about an individual without his prior consent.... Despite these restrictions, the Department is concerned that if the Social Security number were used too broadly, such widespread use and dependence upon the number might lend itself to abuses of individual privacy. Because of this concern, the Social Security Administration is currently reviewing the policies governing the issuance, maintenance, and usage of the Social Security number."
> (Congressional Record, v.115, no. 108)

In a series of hearings before Congress in past years, the Census Bureau has repeatedly testified about questions of privacy. According to Professor Arthur Miller of the University of Michigan:

> "The Census Bureau has an unequalled record among Federal agencies in preserving the confidentiality of personal information; to my knowledge there are no documented cases of abusive handling of an individual's census record."
> (Transcript of "The Advocates", p. 5)

Yet Senator Ervin thought it noteworthy to point out that by 1970 the Federal government's expenditures for statistical data gathering will exceed $200 million including the costs for the Bureau of the Census. He noted that an American is required by law to answer such questions as

> "Do you have a flush toilet?"

and

> "How much did you earn in 1967?"

Another Census Bureau questionnaire asked a sampling of elderly persons such questions as:

> "Taking things all together, would you say you are very happy, pretty happy, or not too happy these days?
> "Do you have artificial dentures?"
> (Congressional Record, v.115, no. 184)

Clearly these questions are of a personal nature and represent an invasion of privacy. To what degree were these people protected? An indication is contained in the Congressional Record, in which the following amazing statement appears:

> "...the Assistant Secretary of Commerce for Economic Affairs, William H. Chartener, ...told the subcommittee that he could not advise people that their responses to a form were voluntary because that would be 'bad psychology." He felt that the Census Bureau had to give the citizen the impression his replies were required on pain of penalty."
> (Congressional Record, vol. 115, no. 184)

(The law requires response only to the national decennial census.)

Concern over invasions of privacy extend far beyond the practices of the government. An especially prominent concern among many members of Congress is the practices of credit bureaus; and for good reason:

> "A visit to any retail credit, bank credit, or legal information bureau on any day of the week can be most revealing (providing the manager doesn't know about the visit). First of all, information in your file contains every negative thing that ever happened to you, going back to the beginning of your credit life. The data is seldom updated, corrected, or weeded out. It includes not just credit data, such as failures to make installment payments on time, but also any legal actions takenaagainst you, divorce or offspring problem reports, newspaper clippings, private detective investigations, FBI or police reports including interviews with gossipy neighbors, etc."
> (Sprague, Richard: "The Invasion of Privacy...")

It is obvious that every American needs to be concerned about invasions of privacy; this subject affects all of us in many ways. We are called upon, almost daily, to make decisions which will affect someone or some organization's privacy. To avoid the problem any longer would be a crucial error and a failure to fulfill our obligation to review questions that are fundamental to the foundations of our nation. We cannot pass off this responsibility to commissions or committees; they can only be participants in the evaluation process. Nor can we dismiss the problem as a simple technological question to be remedied by the scientists -- as Emmanual R. Piore, Chief Scientist for IBM, told Senator Long:

> "...The effectiveness of all protective measures, however sophisticated they become, will still depend upon people.... Machines have no morals, no ethics; men have ethics and morals."

B. What is Privacy?

Lack of widely accepted definition; some insights; four primary functions of privacy; privacy as a biological necessity; constraints imposed by society; constitutional viewpoint vs. moralistic viewpoint.

WHAT IS PRIVACY ?

One might reasonably ask what privacy is and why all these people are so concerned. Privacy is not easily defined; indeed, a widely accepted definition does not exist at this time. However, Arthur Goldberg, former Associate Justice of the Supreme Court, provides some insight into the complex meaning of privacy in a democracy:

> "The fifth amendment privilege protects against more than physical and psychological brutality; it is intrinsic to the individual's right to privacy. The dwindling of privacy has been as frequently noted as the rise of crime. In the modern world, we have only belatedly realized that privacy is an increasingly scarce social resource and one that must be viligently protected against the claims of efficient social ordering."

Another, more functional definition is offered by Congressman Gallagher in his speech before the American Management Association:

> "Privacy can be defined as the free choice by a free man in disclosing to public view and public record certain basic facts about his actions, thoughts, and desires. It is up to the individual to make this decision, just as it is up to those who make the laws to assure that this choice may be made in an atmosphere unclouded by overt coercion or implied threat.... Liberty under law -- the cornerstone of a free America -- demands that the past be a springboard to the full expression and use of ability and not an anchor which pulls a man down and drowns him in youthful mistakes or unevaluated early decisions."
> (Gallagher, March 8, 1968)

These are thoughtful men attempting to determine the true meaning of privacy in a democracy. This is no academic

question; a precise definition would provide a means by which many questions could be viewed -- a moral and philosophical guideline for determining policy and action. It is therefore clear that an additional expenditure of time to further define privacy is well justified.

According to Professor Westin, a democratic society uses publicity as a method for controlling the government and for protecting individuals and groups within the society. He claims that privacy performs four primary functions:

1. Individuals have an intrinsic need for personal autonomy. Privacy provides the conduit through which persons are able to feel that, by the control of information concerning themselves, they have some control over the course of their personal lives. Thus privacy induces independence and diversity of thought.

2. Privacy provides an emotional release; people need to be able to express anger and frustration and to be protected against the ramifications of the publicity of their actions.

3. Privacy provides for self evaluation and introspection.

4. Privacy allows for the protected and privileged transfer of information. It allows one to discuss controversial subjects with fellow employees without the fear of dismissal.

Privacy may very well be a biological necessity. Professor Westin goes on to say that studies of animal

behavior indicate that men and animals may very well share basic mechanisms for seeking privacy within their environment. Writing in Think Magazine, Westin discusses this possibility:

> "Ecological studies have demonstrated that animals also have minimum needs for private space without which the animal's survival will be jeopardized. Since overpopulation can impede the animal's ability to smell, court, or be free from constant defense reactions, such a condition upsets the social organization of the animal group. The animals may then kill each other to reduce the crowding, or they may engage in mass suicidal reductions of the population, as lemmings do." (Westin, Think, May-June, 1969)

Given that man is a much more complex animal, one might extrapolate that privacy is an even more significant determinant of behavior in the human species. Indeed, many studies (including those by Margaret Mead) demonstrate that individuals in primitive as well as modern societies go to great lengths to develop personal privacy for themselves.

Each individual decides upon the degree of privacy he desires. The constraints of institutionalized invasions of privacy limit, to a certain extent, the type and quantity of privacy that he can select. For example, a person may decide to apply for a credit card. This decision means that, although he may not approve of the invasion of his privacy, the agency with whom he applied for credit will find out his salary, his bank account balances, his real estate ownership, his marital status, and considerable other information about his private life. Thus, although he might initially have chosen to live with a great degree of privacy, the demands of the economic activity with which he

has become involved have severely limited his privacy.

However, privacy is more than a credit investigation or job references; it is also the degree to which one's friends'honor the confidentiality of a conversation. It is the conversations which may be monitored by the telephone company (as was done in Washington, D.C.).

Thus it can be concluded that privacy can be viewed from both moralistic and constitutional viewpoints; the moralistic viewpoint includes the individual's personal actions and beliefs as they relate to privacy; the constitutional aspect is that degree of invasion of privacy which our governmental process considers permissible. In the absence of explicit legal evidence, the quality and nature of national moral attitudes will determine the extent to which we violate each other's privacy. The extent of current legal protection, including the complex questions of constitutional law, will be examined in subsequent sections; the current moral situation in the U. S. has been implicitly discussed above, but in the final analysis is left to the determination of each individual in our society.

C. Privacy and the Law

Some legal principles: the Constitution; the First Amendment; the Fourth Amendment; the Fifth and Fourteenth Amendments; credit bureaus; Use of the Courts: difficulties in bringing and winning suit; inherent limitations of the legal system; The Chilling Effect.

PRIVACY AND THE LAW

SOME LEGAL PRINCIPLES

Justice Douglas has said that "the right of privacy is older than the Bill of Rights".[1] The Constitution of the U. S. makes no mention of privacy because the government at that time was far more limited; the problem was having too little information rather than having too much. But as Professor Reich of Yale says:

> "If you read the Constitution in every way in which they understood privacy then, they protected it (privacy) in the Constitution.
>
> "They protected speech and expressions and beliefs, and those it seems to me are illustrations of privacy. They protected religion and conscience, each individual's to be his own.
>
> "They protected against being forced to incriminate themselves by any official body. That is all the invasions of privacy that they knew of in their time."[2]

This is a general problem in U. S. law. Chief Justice Taney stated in Dred Scott vs. Sanford that

> "The Constitution must be construed now as it was understood at the time of its adoption."[3]

Nowadays this trend has changed, and Chief Justice Douglas has suggested that the Constitution is

> "...intended to endure for ages to come, and consequently adapted to the various crises in human affairs.[4]

---

1. 381 U.S. at 486.

2. Reich, Charles A.; statement before Gallagher's committee, 1966.

3. 60 U.S. (19 How.) 393 (1856).

4. McCulloch vs. Maryland, 17 U.S. (4 Wheat) 316.

In 1965, in Griswold vs. Conn., the Supreme Court announced the discovery of a new constitutional right to privacy. Justice Douglas asserted that

> "The right to privacy is a right implicit in a free society; a notion of privacy is not drawn from the blue. It emanates from the totality of the constitutional scheme under which we live."[5]

The Griswold case was an attempt to protect the right of privacy in sexual life, which was not recognized by a Connecticut law which made the use of contraceptives a criminal offense. The law was finally ruled unconstitutional.

The First Amendment has been used extensively and publicly by organizations such as the NAACP to claim privacy of associational life.[6] But in the case of Local 309 vs. Gates, the court has held that two conditions must obtain if an invasion of associational privacy is to be proved:

> "...the actual interference (by the state police when they took notes) and the absence of any right to be in the private meeting."[7]

Neither of these conditions alone is sufficient -- the injunction was not granted simply on account of surveillance. The same case was referred to by the Supreme Court of New Jersey when it held

> "...that the power of surveillance is imperative."[8]

Another interesting strand of possible rights to privacy arising out of the First Amendment is that of a "right to

---

5. 367 U.S. 517.

6. NAACP vs. Alabama 357 U.S. 449 (1958).

7. Local 309 vs. Gates 75F Supp. 620 (N D Ind 1948).

8. Anderson vs. Sills 56 N J 210 (1970).

silence." But efforts to press toward judicial recognition have so far been in vain, since the recognition of such a right would nullify the requirements made of compulsory witnesses.

The witness has a right, however, to avoid self-incrimination, which is granted by the Fifth Amendment. It safeguards not only his privacy, but also that of his family and friends. Brandeis noted that to protect the right to be let alone,

> "Every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." [9]

It would seem to follow that a broad right to privacy is at least equally inferable from the guarantee of "liberty." In the Griswold case, Justices Harlan and White had no difficulty in broadening the guarantee of liberty given by the Fifth and Fourteenth Amendments in order to hold marital privacy to be one aspect of the liberty protected against state action. The enactment violated values "implicit in the concept of ordered liberty." If "liberty" or the "concept of ordered liberty" in the Fourteenth Amendment permits the protection of privacy in general without reference to specific provisions of the Bill of Rights, then it would seem even more logical to ascribe these same meanings to the word "liberty" in the Fifth Amendment. The right to privacy would thus gain independent existence, and would become a concept capable of almost limitless judicial formulation.

---

9. 277 U.S. at 478

The right of privacy is also protected by the right not to be defamed. The Supreme Court, claims Professor Reich,

> "...has recently been extraordinarily scrupulous with respect to the right to have a lawyer and the right to confront."

This could apply directly to

> "...instances of condemnation without trial, of information supplied without confrontation, and of a denial to the individual of any chance whatever to answer." [10]

One very important problem in terms of privacy is the issue of credit bureaus; unfortunately, an Oklahoma Statute[11] is the only legislation, state or federal, which specifically addresses this problem. It concentrates on the issue of access, and makes the provision that a copy of every report should first be mailed to the person about whom it is written. Usually the credit bureau report is conditionally privileged, as recognized by many courts:

> "Thus in the absence of malice, the subject of the report has no cause of action against the credit bureau, regardless of the falsity of the report." [12]

The basis of this privilege is that the credit bureau is performing a necessary and useful business which benefits those who have a legitimate interest in the report.[13] Such a privilege is not recognized in England; we doubt its constitutionality here.

---

10. Reich, C. A., Gallagher's hearings, 1966.

11. Congress, U.S. "Privacy and the National Data Bank Concept."

12. Wetherby vs. Retail Credit Co. 235 Md 237, 201 A2d 344 (1963).

13. Georgetown Law Journal, v.57, no. 3, Feb. 1969.

USE OF THE COURTS

Any U.S. citizen who feels that a law is unconstitutional may attack it before the Supreme Court. Such attacks have been successful in the Griswold case, and have been linked to the change since 1937 in the general view of the role of the Supreme Court.

The federal courts may not be used

> "...as a forum in which to air the general complaints about the conduct of government or the allocation of power in the Federal system."[14]

Thus, a single citizen may have great difficulty bringing his grievance against a federal or state agency to court. However, he may rely on the statement that:

> "...allegations of serious and substantial constitutional violations by government activity present a conflict susceptible of judicial resolution."[15]

But there must be sufficient evidence to render credibility to the allegations.[16] There is a very definite problem for the plantiffs in establishing sufficient evidence.

Before the courts will accept a case, the plaintiff has to prove (according to 28 U.S.C. 1331) that his civil action involves controversy in an amount of over $10,000.[17] The plaintiff must have justiciability; that is, he has to demonstrate that the following are judicially identifiable:

---

14. Flast vs. Cohen 392 U.S. 83 (1968).

15. Stamler vs. Willis 415 F 2d 1365 (7th Cir. 1969).

16. National Student Assoc. vs. Hershey, 412 F 2d 1103 (1969).

17. Giancana vs. Hoover 322 F 2d 789 (9th Cir 1963).

a right in the plaintiffs, a duty of the defendants, a breach of that duty, and a remedy within the power of the court. "A right in the plaintiffs" and "a duty of the defendants" both give way to the same problem of the availability of judicial proof and evidence. The "breach of duty" is even more difficult to prove. As the plaintiffs of Arlo Tatum vs. Melvin Laird said,

> "There is a threat of unknown surveillance, unknown purpose, and unknown future use of the information gathered and recorded."[18]

How can you bring evidence of the unknown?

The defendant will often claim that

> "...the basic approach must beethat the executive branch may gather whatever information it reasonably believes to be necessary to enable it to perform the police roles, directional and preventive."[19]

But the problem with this, as Professor Reich says, is that it is easy to tell what information would be useful, but it is not easy to tell what is necessary.[20] This is yet another obstacle to proof of "breach of duty."

The plaintiffs also have to prove that the remedy is within the power of the court. In dealing with the executive branch, the plaintiff runs head on into the doctrine of separation of powers -- the case itself may be unconstitutional.

---

18. U.S.C. no 242203.

19. Anderson vs. Sills, N. J. Supreme Court, June 2, 1970.

20. Reich, C. A., Gallagher's hearings, 1966.

It therefore proves very difficult -- if not impossible -- for the private citizen to win in court on the grounds of invasion of privacy.

From a practical standpoint, this state of affairs is beneficial to the legal system: it is doubtful that the Justice Department would be prepared to handle the number of cases which would arise if such technical barriers did not exist. A trend toward elimination of such barriers is becoming evidenced in the lower courts (as in Anderson vs. Sills), but these decisions are still being reversed by the higher courts.

If in fact the plaintiff is able to overcome all these obstacles and present his judicial evidence, he will be suprised to learn how the Consent Placebo is used by the courts: the plaintiff will be assumed to have consented

> "...to the dissemination of personal information or waived his right to protest by engaging in activity inconsistent with a desire to maintain privacy. Unfortunately, the application of both of these concepts by the courts has been somewhat Draconian."[21]

The whole ideas of "consent" and "waiver" are defined without reference to the context of the specific situation. It seems rather illogical to say that a person who is in court fighting for his right to privacy consents to abandoning that right.

Modern technology and the advance of new ideas and ideals threaten to make our judicial system an anachronism. Privacy

---

21. Miller, Arthur, Michigan Law Review, April 1969.

is not a problem which the court system is technically competent to handle. Indeed, the law itself seems unable to handle problems based on non-concrete concepts -- how do you place a dollar value on an individual's right to privacy so that you can decide whether it is worth more than $10,000?

THE CHILLING EFFECT

The value of the right to privacy includes more than the amount of money a person lost through being denied a job or credit for invalid reasons; it includes the social cost of the erosion of the civil liberties which are the fabric of democracy. The chilling effect on civil liberties is not an imaginary problem; it is an important threat to our society. As Justice Robert Mathews of the New Jersey Supreme Court has said:

> "Information gathering can have a chilling effect on anyone advocating social and political change because of involving his wife, his family, or his employer."[22]

The chilling effect doctrine -- based on the First Amendment -- began in 1947. Some civil servants attacked one of the Hatch Act's provisions; under which they had been threatened with dismissal from employment. The court ruled that

> "...the general threat of possible interference with those appellants' rights by the Civil Service Commission under its...rules does not make a justiciable case or controversy. A hypothetical threat is not enough."[23]

---

22. Anderson vs. Sills 56 N.J. 210 (1970).

23. United Public Workers vs. Mitchell 330 U.S. 75 (1947).

But in 1965 the court recognized "the chilling effect on the free expression of prosecutions initiated and threatened."[24] Conversely, in 1968, the court refused to enjoin the enforcement of an anti-picketing law and said:

> "Any chilling effect on the picketing as a form of protest and expression that flows from the good faith enforcement of this valid statute would not of course constitute that enforcement an impermissible invasion of protected freedoms."[25]

The chilling effect doctrine was most significantly stated in 1969.[26] The Hershey directive called for the reclassification of war protesters as a result of their exercise of the right of freedom of expression. In view of the obvious effect that the policy would have on young men who might otherwise voice dissent, the Supreme Court held that the policy was contrary to law. The guidelines by which a given chilling effect may be ruled unconstitutional are:

> "1) The severity and scope of the alleged chilling effect on First Amendment freedoms.
> "2) The likelihood of other opportunities to vindicate such First Amendment rights as may be infringed with reasonable promptness.
> "3) The nature of the issues which a full adjudication on the merits must resolve and the need for factual referents in order properly to define and narrow the issues.
> "These issues become relevant of course only if the plaintiff plausibly allege that they are in fact vulnerable to the alleged chilling effect."[27]

---

24. 380 U.S. at 487 Dombrovski vs. Pfister.

25. Cameron vs. Johnson 390 U.S. 611 (1968).

26. National Student Association vs. Hershey, 412 F 2d 1103.

27. 412 F 2d at 1115.

Here again the problem of judiciable evidence arises because the chilling effect is a threat and a fear of the unknown. Once again the enforcement of a law on privacy is prevented.

D. How privacy is invaded.

Asking questions; readily available public sources; complete physical and psychological surveillance.

HOW PRIVACY IS INVADED

The means by which privacy is violated are numerous and varied; they range from unsophisticated to highly technical methods.

The most obvious means to obtain information from people is to ask them questions. Surprisingly, very few people refuse to answer questions on such topics as income, sexual behavior, political and religious beliefs, and educational background, if only the questions appear in some "legitimate" form (i.e. questionnaires, voter opinion surveys, and the like)) People are equally willing to divulge information about the drinking habits and marital behavior of their neighbors. It is clear that too few people question the validity or necessity of the process requesting information from them before discussing their personal affairs. Simple questioning without coersion or pretext is the major means by which invasion of privacy occurs.

A second technique for obtaining information, which entails a greater degree of risk in some instances, is to search readily available information such as town records and published information including books, newspapers, and unofficial reports of various organizations. Sometimes information must be purchased if this technique is utilized. For example, the Internal Revenue Service has had a policy of selling to anyone lists of all persons in the U.S. who own

registered firearms. But more often than not the information is available, for all intents and purposes, for free. The Soviet Union, a number of years ago, desired to obtain data that would thoroughly describe the Baltimore harbor -- information of obvious strategic importance. They were able to purchase from the U.S. Government, for a nominal fee, comprehensive books detailing all the information they wanted and more about not only the Baltimore harbor, but about all major eastern harbors. This saved them an estimated two million dollars in spying efforts.

Sometimes this method of information retrieval is more risky. Intelligence agents or the curious seeking information at such places as universities have been known to employ a diversionary tactic if refused access to information -- one person diverts the clerk or secretary's attention while the other looks up the necessary information. The willingness of people to divulge information, however, means that this technique is usually unnecessary. In any event, the utilization of existing stores of information is the second major source of data by which privacy might be invaded.

The third and less frequently method of information collection is physical and psychological surveillance. This involves the use of manpower and at times electronic equipment to monitor a person's activities, conversations, associations, and practically every other aspect of his life.

The discussion now turns to the utilization of modern science to gather and store information. First considered are a few of the many ways in which science allows

us to covertly collect data on our fellow citizens. Then the impact of the electronic computer on our ability to store, retreive, process, and disseminate that data is examined.

E. Privacy and Technology

Electronic spying devices; counter-surveillance measures; the sellers and buyers; the computer and invasion of privacy; access control and security in time-shared computer systems.

PRIVACY AND TECHNOLOGY

METHODS OF ELECTRONIC SURVEILLANCE

In order that the reader not be permitted to think that electronic spying is an activity confined to James Bond movies, presented here is a description of the most commonly available electronic data collection devices, along with details of who buys and sells them. This section should be read with two facts in mind. First, the data is from a book published in 1967 (Brown, The Electronic Invasion), and technology has at this writing three additional years of constant advance. Second, the devices discussed are ones available to anyone who has the means to pay for them; no mention is made of any top secret devices. It has been said that the National Security Agency normally uses equipment with a technology level ten years ahead of that available to other consumers.

Electronic bugging first came to the public eye in 1960 when Henry Cabbot Lodge revealed to the United Nations that the USSR had bugged the great seal of the United States in the office of the U.S. Ambassador to Moscow. The device consisted of a very simple resonance chamber with an amplifier that could be picked up for a few hundred feet. Since that time considerable sophistication has been achieved. A manager in one company who was interviewed by Mr. Brown was reminiscing about the old days when bugs

were big devices with wires and batteries which put out so much heat that they could not be concealed except in very large hiding places. Moreover, the spy was lucky if the broadcast reached the next room. On the executive's desk was one of the company's more recent devices. It was less than an inch in all dimensions, and was designed to be implanted in a chimpanzee for the purpose of sending data on weightlessness back from a satellite.

By far the most common exercise is to bug a suspect's telephone. The classic picture is that of two bored detectives in a small room listening to a set of earphones for hours in case someone makes a call. Today, however, the bugs transmit directly to tape recorders, and they turn themselves off and on when calls are made. The broadcasting portion of the automatic bugs is available at a cost of 50¢ and up.

Of course, an ideal phone tap would be one that can not be identified as a tap even if found, that picks up both sides of a conversation, and that requires no direct connection to the telephone. In fact, Consolidated Acoustics sells this device, disguised as a diary, for $59.50. It must be within three to four feet of the telephone (in a desk drawer for instance), and will broadcast over a range of two city blocks.

For the unsophisticated tapper, the carbon button inside the speaker of the phone may be replaced with an

identical (but bugged) copy. Installation requires less than ten seconds, and the telephone company has been baffled for considerable periods before detecting it. It costs $244.50 from Micro Communications Corporation, but Tri-tron sells it for $169.95.

If replacing the button is still too much work, Continental Telephone sells a pre-bugged phone complete for $250. It is available in touch-tone and colors.

All of these devices suffer from limited broadcast range. Therefore, the best phone bug of all is the Harmonica bug, which has unlimited range. The harmonica bug is available from Miles Wireless Intercom, Ltd, for $700 or from Emmanuel Mittleman of New York for $400, and it must be installed inside sthe telephone. In addition, the tapper must be prepared to purchase a Holner key of C harmonica (about 45¢ at the five and dime). He then goes to a phone from which he wished to tap and dials the number of the bugged phone. Blowing a specific note on the harmonica activates the bug, which turns off the bell on the victim's phone, connects his receiver, and amplifies the pickup so that any conversation in the room is audible. The bug disconnects in the event that the victim picks up the peneiver to dial out. The same device can be had from Continental Telephone, with an oscillator substituted for the harmonica, for $1000.

However, efficient eavesdropping requires the ability to do more than bug telephones. Next considered are mikes

and miniature amplifiers.

The most popular of these, in the movies,, are the sugar cube bug and the martini olive bug. The device used is actually smaller than a sugar cube (1" x 3/4" x 1/4") and sells from Continental Telephone for $149.95 (ask for the Micro 007). In reality, however, the sugar-cube-and-olive ploy is very poor and is infrequently used. In the first place, the devices broadcast range is only 200 feet. Moreover, the olive looks like an olive only after a substantial number of martinis, and can be disabled by simply removing the toothpick. The sugar cube must also have an antenna which is difficult to disguise; if it is suspected, victims should endeavor to accidentally tip their water glass into the sugar bowl.

Much nicer than these are the wide range of small mikes which are imported by Telephone Dynamics Corporation and Continental Telephone. These include the buttonhole mike and the tie mike ($15 to $39.95).

Along these same lines, but a little larger, are a mike the size of a hearing aid for use under carpets, etc., which sells from Consolidated Acoustics for $2.25, and a variety of mikes with transmitters disguised as various desk implements. One of these is even built into a fountain pen, so that the spy may take notes while he records.

The snake mike (Continental Telephone, $119.50; Tri-tron $37.50) consists of a flexible acoustical tube which is

extremely difficult to detect and may be unrolled like fish line through a skylight or keyhole. It is obviously useful only for very specialized operations.

A variety of other mikes are available in all sizes and shapes. At least one is available for every conceivable operation. For a fuller discussion, the reader is referred to Mr. Brown's book.

Moving on to bigger bugs, the next class of devices are useful for bugging whole rooms. These include the spike mike (built into a spike, so that it can be nailed into the victim's wall), and a variety of cigarette-package sized mikes priced from $49.50. The most exotic of these are:

-The fountain pen bug mentioned above. It costs $179.95 and may be charged on your Diner's Club card.

-The whisper light, a pre-bugged lamp useful for marital cases, which is usually presented to the victim as a gift for his bedroom ($150.)

-The picture frame bug, available from Continental for $150., and from Mosler Research Products for $215. It has the advantage of being quite large, so that long-life batteries may be installed, and is said to be quite tastefully designed. It may be purchased either with or without a painting.

It should be noted that a problem with room bugs is that their batteries eventually run down. One of the cleverist

of the bugs, therefore, is that available through Steckler Sales of New York. It is activated by voices ortother noises in the room, and turns itself off when there is nothing to listen to in order to conserve power.

COUNTER-SURVEILLANCE MEASURES

With so many people interested in listening in, then there must be someone interested in keeping them from doing so. The market in bug detectors and disabling devices is much less well developed; nonetheless, there exist some devices which are useful.

The most naive method of bug detection is to use an FM radio and/or your television set to set up feedback patterns for local bugs. By tuning slowly toall available stations, feedback can usually be obtained on the appropriate wavelength or one of its harmonics. Some bugs exist that cannot be detected in this fashion.

Perhaps the most sophisticated device is a beep light, available from Dee Company for $195 to $295. This device can be set to signal whenever radio transmission is occurring nearby, and can therefore be constantly on guard above your office door.

For those who would rather defeat the bugs than find them, a variety of scrambling devices are available ($550 and up) for telephone conversations, and a number of jamming devices may be had to foil other bugs. The jammers have the unfortunate side effect of ruining your television and radio transmission, however, and at one time were so

powerful as to interfere with communications of airplanes flying overhead.

THE SELLERS AND BUYERS

It should be clear that this market is widely developed because of a great demand for such products. Mr. Brown lists some seventy-one companies which are involved in the bug market to a greater or lesser degree; it is not instructive to describe them in detail here. However, a brief look might be given to some of the buyers. The government buyers include the IRS, NASA, the Atomic Energy Commission, Bureau of Customs, Bureau of Narcotics, FDA, General Services Administration, the U.S. Information Agency, the Secret Service, and the Treasury School. Moreover, every army intelligence unit is capable of wire-tapping, although our findings indicate that they leave such tasks to the local police and FBI, who specialize in such things.

Industry buyers include Alabama Gas Corporation, American Airlines, Avis, Boston Gas, Chrysler, Coca Cola, Encyclopedia Americana, Hertz, Philco, Prudential Insurance, and Walt Disney Productions.

Indeed, industrial espionage is at least as big a business as government domestic espionage. A study performed by Saber Laboratories, which specializes in anti-bug devices, reaches the following conclusions with regard to industrial espionage:

-It takes place where there is high competition.

The threat in the automobile industry is 100%.

-Its goal is the same as foreign espionage.

-Its tools are also the same,-- booze, broads, blackmail, bribes, and bugs.

-Annual losses due to industrial espionage were conservatively estimated (1967) to be three billion dollars.

-Only six percent of non-defense industries are capable of detecting espionage.

-Only five percent of law enforcement officials are capable of detecting industrial espionage.

It is hoped that these facts sufficiently alert the reader to the latest methods for collection of data on individuals and groups without their knowledge. The discussion now turns to the most powerful device yet invented for processing that data -- the electronic computer.

THE COMPUTER AND INVASION OF PRIVACY

It is possible that the computer is the most powerful tool ever developed by man; yet it is still a tool in exactly the same sense that the hammer is a tool. The hammer amplifies man's ability to strike; the computer amplifies his ability to process information. By doing so, the computer can be made to amplify man's ability to think.

But tools are amoral objects. There is nothing inherent in a hammer to force it to hit nails rather than another man's head. In the same way, the computer is amoral. It is only one kind of amplifier for man's ability to do good or evil. Our concern should be greater, however, for

the computer than for the hammer because of the greater magnitude of the computer's amplifying power. As Congressman Gallagher put it:

> "...It would probably take all the people in America working 10 hours a day, five days a week, to duplicate the output of government computers.
>
> "Yet, it must also be remembered that 100 clerks working around the clock for 100 years may not be able to make the number of mistakes a computer can make in 1 minute."
> (Gallagher, May 7, 1968)

The computer does not invade our privacy; it only takes the information given it and does what it is told to do. Men invade our privacy. However, the power inherent in the computer to propagate that invasion of privacy staggers the mind. Some examples of currently existing technology serve to demonstrate that power.

First, in terms of processing speed, consider the IBM 360/195. It is capable of performing on the order of twenty-five million calculations per second.

Second, in terms of storage capacity for information, consider the mass storage unit now marketed by Precision Instrument Company of Palo Alto California:

> "This system uses a one-watt, continuous-wave argon laser to burn minute "pits" in the opaque coating of plastic computer tape. The laser is so precise...that each pit is only one micron, or .000039 inch in size. Where normal recording has been about 5600 bits of information on an inch of magnetic tape, the new laser process can put 645,000,000 bits in microscopic parallel rows on each inch. And the recording process achieves speeds of 12,000,000 bits per second.
>
> "...In terms of a dossier society, the laser memory system means that a single 4800-foot reel

> of one-inch tape could contain about 20 double-spaced typed pages of data on every person in the United States -- man, woman, and child. It would take only four minutes to retrieve a person's dossier under such a system."
> (Congressional Record, Apr. 25, 1968, p. E3359).

Lastly, consider the computer's ability to communicate its information to man. Line printers are commonly used that output at the rate of 1000 lines per minute. Since this is extremely slow with respect to processing time, a single computer will often run many of these printers simultaneously. For those who consider this rate still too slow, a variety of other devices, such as a direct microfilm printer, are available. Moreover, the idea of the computer for everyman, with terminals in each home, is not far removed from the realm of possibility; a number of firms now sell typewriter-like terminals that may be attached directly to the standard home telephone. They can communicate with any computer in Ma Bell's domain.

Perhaps the greatest public concern has been caused by the advent of multiple-access time sharing systems, in which a rather large number of users are utilizing one computer simultaneously. It is indeed clear that these systems present a much greater threat to privacy than even the batch systems of past years. Problems of controlling access to information stored on-line are greatly complicated when forty persons are using the same physical devices at the same time. However, time-sharing hardware and software also present much better opportunities for access control than conventional systems. The technology for protection currently exists, although it is not commonly used in business or government.

ACCESS CONTROL AND SECURITY IN TIME-SHARED COMPUTERS

The first problem is identification of the user at his terminal. Since the terminals are remote from the computer itself, it is much more difficult to find out if the user is who he says he is. The only commonly used method of identification is the password, and commercial and government systems vary greatly in the sophistication of their password schemes. In any case, the user is required to supply a more-or-less secret password at the time he logs in. Some of the problems with such a scheme are obvious. Aside from the possibility of coersion of a user to obtain his password, there is the possibility that someone will obtain access to the entire system password file, either through electronic means or by bribing system operators. Therefore, a number of other schemes have been proposed, ranging from fingerprints to signatures. Most of these schemes are technically feasible; however, they fail to realize that any identification must be transformed to a bit pattern for transmission to the computer. No matter how complex the identification technique, the user's i.d. can be had for the trouble of tapping the line and recording that bit pattern.

What is needed, therefore, is an identification scheme that varies dynamically over time. Such a scheme, now in use by the Project MAC Advanced Interactive Management System (MacAIMS) at M.I.T., is the procedural password. In this method of identification, the

computer prompts the user with a string of random digits (different at each log-in). The user then performs a simple calculation (the procedure) on the digits and returns an answer, which may be arbitrarily disguised, based on that calculation. The correctness of this answer determines whether access is permitted. Thus, since the prompting number is different each time, the password is also different. Each user, of course, has a different procedure for obtaining the answer. Unfortunately, it could be coereed from him.

The next problem is that of tapping of communications lines between the computer and the terminal. All major time sharing systems in use today transmit over standard telephone company lines. There is no way that thettapping of such lines can be prohibited. However, it is possible to construct lines which are arbitrarily difficult to tap without being detected. Unfortunately, the telephone company has no thought of ripping out all their currently existing lines to replace them with more expensive ones. Moreover, the cost of running special lines for an individual system is almost always prohibitive.

The only solution for transmission security that is practical today, therefore, is the encoding of the information transmitted. It is clear that coding schemes of arbitrary complexity can be thought up and changed at will. The cost of such schemes in terms of reduced processing speed caused by the necessity of coding and decoding each piece of data, and in terms of the necessity to have decoding logic built

into each terminal is so great that encoding schemes are not commonly used.

Once inside the computer, the access control problems are those of deciding how to store information in such a way that willful or accidental misuse of the data may be prevented. In Multics (The Multiplexed Information and Computing Service of Project MAC at M.I.T.), for example, each user has the ability to store his data in separate units called segments, and to specify who may (or may not) have access to each of those segments. A variety of access modes (i.e. access to read, to write only, to append, etc.) are provided, and the user may change the access control lists of his information at will. Every attempt to access a segment is checked against the access control lists before access is permitted. Thus the access control lists may be used to prevent unwanted invasions of the storage system.

Multics has also implemented a ring structure for protection, which may be viewed as a number of concentric rings of privilege. The operating system decides in which ring a particular program may execute, and any program which tries to reference an inner ring will be trapped by the supervisor. Thus at the time any access to a more privileged ring is attempted, the programs in that privileged ring have the option of deciding whether to permit access. Thus "access" does not mean unlimited privileges -- access to a user's data may be completely under the control of his own programs.

A related problem which is being studied in detail at MacAIMS is the question of how to decide who may have access to output information which has been aggregated from input information with specific access characteristics Solutions to this problem should be forthcoming in the near future.

Thus, as the Multics example show, a large variety of technical solutions to access control problems are currently available. However, these solutions are not widely implemented in any area except the academic environment of M.I.T. It is implicit in the above statements that one reason for this lack of use of protection schemes is the cost involved. Multics and other systems have shown, however, that the cost of protection is not prohibitive. But since the builders of computer systems are almost never the same group as those whose privacy is threatened in a direct manner by the system, the incentive to incur that cost is very low. In fact, in many cases the incentive is quite negative. Consider for a moment the size of the power gap that may exist between the controllers of information and the people to whom the information pertains. The truism that private knowledge is power is indeed quite strue. An unfortunage fact of human nature is that there are very few people who, having once experienced power, prefer having less of it sto having more.

However, the main reason for the wide-spread lack of adequate protection is probably that the state of the art in computer science in areas outside the academic sphere is far

less advanced than the examples discussed. Many, if not most, of the computer users in government and industry are still trying to get their machines to process data at all. They have not yet reached the point of trying to process data well. Moreover, many computer manufacturers also lack the necessary sophistication -- for example, the IBM System 360 lacks the hardware to inhibit reading.

In the final analysis, then, computers need not be the problem. It is much easier to set up a system for access control in a centralized computer file than in decentralized hand operated systems. Computerized access control, however, depends very heavily on the availability of honest and very competent programmers. The implementation of a system like Multics requires a tremendous effort.

Centralization of information in a computer makes many operations cost-effective that would otherwise be unreasonably expensive. Unfortunately, the fact that the access system becomes centralized also makes concentrated efforts to break the access controls cost-effective. Centralization of sensitive information can therefore be expected to cause an increase in determined attacks on the access control mechanisms, and any decision to centralize information must take account of this increase. The security of the access control system becomes a very important issue.

Ultimately, the implementation of proper security measures in computer systems is the responsibility of the systems designers. A variety of measures may be taken to protect

against the System Administrators. One might, for example, partition the system development effort in such a way that no single person would know enough to violate privacy measures. One might require certain decisions to be made by groups of people rather than by one individual. One might have extensive auditing procedures analogous to those used in accounting practice today. Essentially none of these measures are in use today.

Not all of the technical difficulties related to protection have been solved; however, the technical capabilities to make the computer an amoral tool to a large extent exist today; It is the human problems upon which we need to concentrate most. There can be no question but that our privacy is threatened virtually every day. The advanced state of our technology combined with the willingness of citizens to divulge information about almost any individual can be obtained if one is willing to make an effort to do so. Unfortunately, very few safeguards exist to regulate either who collects information or how. And many people are willing to make a considerable effort to collect information on all of us, sometimes for very valid reasons, occasionally for not so valid reasons.

b. An initial solution and its shortcomings

Allowing individuals access to their own files; reasons this is over-simplistic; conflicts of privacy; first cut at a reasonable solution.

AN INITIAL SOLUTION ANL ITS SHORTCOMINGS

Today the most commonly proposed solution to issues of invasion of privacy is simply to allow individuals access to their own files in order that they might correct any information which is erroneous. This proposal is over-simplistic on several counts:

First, it assumes that the individual is the only entity which might ever be harmed by invasions of privacy. This is, of course, not the case. Even now there are many groups who have been harmed by the illegitimate release of information about them -- large corporations, draft-resistance groups, political groups, and the government itself. These groups presumably have some right to privacy, although Constitutional guarantees are even less well defined than for individuals, and should be given consideration. It is true, however, that the individual remains the most important of these entities in terms of privacy issues.

Second, individual access assumes that the individual is the most qualified person to correct his own record, and that he will be interested in having his file correct. Again, this is in many cases false. It is ridiculous to think, for example, that a person should be able to change his medical record at will; surely we cannot all be physicians. Also, in the case of information which in some way unfavorable, (which is the only information involved in this controversy),

it will never be in the individual's interest to have correct information in his file. If we do not trust a small group of people to accurately report sensitive information, then we surely do not want to have to trust everyone to perform the same function.

However, the most important shortcoming of this method of quality control is that it does not recognize the problem of conflicts of privacy. Most, if not all, of the data with which we are concerned is the joint property of at least two parties -- the person who originated the information, and the person who the data is about. In many cases, the privacy rights of these two individuals are in conflict. Consider, for example, the case of medical records. Included in these records are many impressions that the doctor might note down to aid himself in future work with the patient. For example, it might be very important to remember that a patient shows signs of schizophrenia. However, the doctor would clearly not want the patient to be aware that this opinion was contained in his medical record. Thus, to release the medical record to the patient would conflict with the doctor's right to privacy.

The first cut at a solution to the problem of conflicts of privacy might be to draw a very clear distinction between information which is to be considered fact, and that which is to be considered opinion. In the medical example, it would be possible to separate the facts from the doctor's opinions, giving patients access to the former record but not the latter.

Unfortunately, this distinction between verified fact and heresay opinion is not drawn in many of the important collections of information in use at this time. Moreover, even if it were drawn today, there still would remain a number of true conflicts of privacy which require other methods of resolution.

Thus allowing individuals access to information about them is not an acceptable solution to all questions of invasion of privacy. It is a simplified solution which is, in the final analysis, only applicable to simple cases.

G. The case in favor of data banks

Three main forces driving the collection and dissemination of information; common abuses.

THE CASE IN FAVOR OF DATA BLANKS

All of this, of course, is not to imply that society has no right to collect and dissiminate information regarding individual members or groups of members. Indeed, one of the few characteristics that sets us apart from the lower animals is our ability to record and transmit information from generation to generation by other than genetic means. It would be ridiculous to even consider attempting to run a society without suchiinformation. The question, then, becomes: what limit is to be placed on such collection?

Logically, there are three main forces which drive man to collect data and dissiminate information. The first, and perhaps most prone to abuse, is to facilitate the management function of the society. In order to maintain what we call civilization, a tremendous coordinating effort is needed. For example, much detailed information about an individual is necessary to simply process his paycheck. It is necessary to know his name in order to write the check, his social security number in order to withhold taxes which he is bound by law to pay, his rate of pay in order to calculate the amount of the check, etc. It is difficult to quarrel with the necessity for keeping this information.

Another example of information which is relevant to the management function is the selective service system. Here again, considerable personal information about individuals is

necessary to determine their obligations for military service. It is easy to think of more examples.

The most common way that the necessity for collection of data to perform the management function is abused is by over-extension. The collection of information, as we shall see, has a very powerful driving force inherent within itself. Data collection systems, if left alone, will often collect data far beyond their true needs and collection will become a goal in itself rather than a means to a specific end.

The second driving force for data collection is to set up systems for resolving conflicts in the rights of individual members of the society. It is difficult to think of a right that cannot be abused by specific individuals. For example, it is clear that driver's licenses are necessary in our society to prevent dangerous, incompetent, and reckless persons from abusing other people's rightsto use our roads with some measure of safety. Another good example is the FBI fingerprint file, which is tremendously helpful in preventing the destruction of life and property by criminal elements.

Perhaps the most common way in which data systems set up for resolving such conflicts are abused is that in some cases the resolution of a specific conflict may depend on the relative political power of the individuals or groups involved in the conflict. Such systems must be cautiously constructed to avoid the possibility of might being right.

The last major reason for the collection and dissimination

of information is the value that information has in its own right. Knowledge is power, as the saying goes. It is very difficult to imagine that we could have progressed to our current level of civilization without having institutionalized the public library.

However, in systems which are built for the purpose of dissimination, care must be taken that information is not inappropriately dissiminated. For example, the library should not open its files of individual users' borrowing records to examination by the general public. Moreover, it is important that information systems set up primarily for one of the other two functions be prevented from distributing information for the value of its dissimination; such distribution is almost always inappropriate. Care should be taken, for example, that information from court probation records is not sold for money or favors to prospective employers.

H. Criteria for evaluation of individual data banks.

Criteria for entry into the system; quality control of input data; outdated data; aggregation of data into useful information; access to information; exchange of information between data banks; social benefits vs. social costs.

CRITERIA FOR THE EVALUATION OF INDIVIDUAL DATA BANKS

Based on the above discussions and on the inherent purpose of an information system -- to collect raw data and process it in some way to produce relevant analysis -- it is easy to set down the dimensions upon which any proposed data bank should be evaluated before it is established. Unfortunately, none of these data banks we have investigatedsshow significant signs of being planned with these dimensions in mind; to the extent that the issues have been considered at all, they have come under study only belatedly, after someone important (or loud) has brought theddata bank to the public eye. The five specific dimensions that should be considered are discussed below.

Of primary importance is the criteria by which some piece of datum concerning an individual or a group becomes qualified for entry into the data bank. In order to establish a comprehensive and logical set of criteria, prior thought to the specific goals of the system must be given. If the desired output of the system can be stated precisely (and justified on the basis of the right of individuals and groups to control their own privacy), then input criteria can be defined and bounded in a fashion that not only eliminates the gathering of useless information and promotes efficient system design, but also prevents ill side effects of the data bank on either the individuals with which it is directly concerned or on those

with which it is not concerned.

Most of the intelligence data banks we have investigated either do not have any clear cut criteria for the collection of data or do not follow them. The rule seems to have been to collect anything that happened to come to the attention of the data collection portion of the system, on the chance that it might be useful.

Once reasonable standards have been set up for determining what data is to be sought (and accepted) as input to the system, it is necessary to set up procedures for controlling the quality of that information. Quality control has two aspects. First, there is control of the accuracy of input data as it is entering the system. In a computer system, this might involve checking punch cards forkkeypunching errors; in a standard security check system like the Army's, it might involve careful and extensive training of the collecting agents to discern truthful answers from false ones. Moreover, it should involve distinct separation and labeling of "fact" from "opinion" as discussed above. The systems we have studied have in general failed to perform adequate checking of input data; army investigators, for example, currently receive between two hours and nine days of training in loyalty adjudications before they are sent out to judge security which determine whether the individuals involved can have a job. Included in the nine day course is forty hours of training in typing. Until recently, the practice was followed

of including with the facts collected by these agents spot reports from field men. Spot reports are verbal reports by an agent covering, say, a demonstration which range from two or three words to a short paragraph, and are not verified at all.

The second aspect of quality control concerns the removal of information from the file when it becomes outdated. Until the recent public outcry, none of the data banks investigated ever removed any information of any kind or quality from their files. Today the army has a standing order to destroy spot reports within 60 days after the end of the situation to which they refer. There are a number of exceptions by which such reports may be maintained past this period, and we have not verified the extent to which the standing order is followed at the local level.

The next important consideration is the methodology jused for aggregating all of this raw data into useful information. The collection of data by itself produces very little in the way of predictive information; relevant portions of the data must be combined and analysed by more or less sophisticated techniques. Many of the failures of prediction of current data systems result from a lack of understanding of this very basic difference between data and information; data are the building blocks from which information is obtained.

Given a system which is able to provide useful information, it is necessary to very carefully control access to that

information. Access control is a necessity that goes far beyond intelligence files; virtually every piece of information that is useful is sensitive to a greater or lesser degree, and must therefore be protected. Very specific rules for the dispersal of information from a system must be set up. These rules must consider both the authority and the need to know of the potential receiver of the information. Such rules are, of course easy to conceive. Seeing that they are followed is quite another matter. Codes can be broken, employees can be bribed, and any number of more or less covert techniques applied in order to circumvent rules which have been established. Thus, access control must include mechanisms for determining when access rules have been violated -- this is the issue of security. The most simple-minded security measure (simple because it is also very susceptible to violation) is the audit trail.

A sub-problem of access control is exchange of information (or data) between data banks. Not only must care be taken to insure that such exchanges are appropriate in terms of the rights of the individuals or groups to which the information pertains, but also greater scrutiny than ever is required to verify the accuracy of information obtained in such an exchange. One argument for preventing or minimizing the exchange of information between systems is the hope that by maintaining separate systems, the biases associated with each collection and analysis scheme will cancel each other out, and thus pro-

vide the decision-maker with a more balanced picture of the real situation.

Last and most important, consideration must be given to the social effects of the proposed information system. Each function that the system is to perform must be weighed in terms of its social benefits and social costs. The benefits may be delineated in terms of the driving force behind the system's establishment -- will the system in fact assist in the management function of the society; or will it help resolve conflicts of individual's rights; or will it cause progress through the distribution of knowledge?

These benefits must be balanced againsttthe social costs of the system, which may be measured in terms of the individual's loss of privacy, the resulting degradation of freedom and the possible chilling effect on the exercise of civil liberties.

PART III: THE DOMESTIC INTELLIGENCE COMMUNITY; ITS COLLECTION OF INFORMATION ON LAWFUL POLITICAL ACTIVITIES

A. Justification for political intelligence files and their inconsistencies.

Deterrent power; apprehension of criminals; necessity for preparedness; public nature of public actions; nothing to hide; shortcomings of these arguments.

JUSTIFICATIONS FOR POLITICAL INTELLIGENCE FILES AND THEIR INCONSISTENCIES

We now turn to an examination of the most prominent justifications given for the maintenance of intelligence files on dissidents engaged in lawful activity. It should be noted that, in this context, justifications are different from reasons for establishment. Our research reveals no substantial attempts to justify the creation of such files to proper authorities (i.e., authorities at the appropriate levels to make policy judgments concerning the right of the American people to privacy) at the time the files were established; these justifications have been brought forward only in the face of public outcry against the files.

The first benefit cited for the maintenance of such files is that they serve as a deterrent to would-be criminals. Presumably, such deterrent power rests on the general public's knowledge of an effective and powerful police force, armed with the knowledge to track and apprehend criminal offenders of all varieties. For example, Florida Chief of Police Bernard Garmire has said:

> "It's absolutely imperative that the police do it (maintain files), Sir.
> "...To prevent crime; to protect the rights of the people...; it's incumbent upon the police to know what's going on their respective jurisdictions....
>
> QUESTION: So you in effect can watch anyone in the United States at your discretion?
>
> Garmire: I think so, yes, Sir."
> (Transcript of The Advocates, Oct 27, 1970, p.16-17)

However, it should be noted that very few concrete examples of the prevention of violence based on the existence of the files have been given. Many proposed examples on closer examination are revealed to be cases involving known criminals or persons engaged in clearly illegal activities. Such cases are not to the point of the scrutiny of legal activities. Chief Garmire proposes one case in which the bombing of Key Biscayne by a person who had no previous criminal record was prevented:

> "We apprehended, in the city of Miami, a young person who was actively attempting to enlist and recruit the support of people who had technological ability in the construction of bombs...."
> (Transcript of The Advocates, p.16.)

But the making of bombs is not a legal activity. Most examples show similar deficiencies.

Moreover, there are numerous examples where such surveillance has not prevented violence. Paul Weaver, a Harvard professor who appeared on "The Advocates" in support of the maintenance of the files, has admitted:

> "I don't know of any evidence that surveillance directly deters assassins or disorderly disruptions or anything that is illegal or violent...."
> (Transcript of The Advocates, p.

Almost any riot or violent demonstration in the last few years can be used as an example of a case where extensive surveillance has not prevented violence.

Professor Weaver has said in a personal interview, however, that he considers the deterrent effect of such files to be an unmeasurable quantity. It is impossible, he claims, to set up a properly controlled experiment to

test whether more or fewer acts of violence would occur in the absence of such surveillance.

The second benefit cited for the files is that they are an aid to the apprehension of criminals who have in the past committed crimes. Examples are the apprehension of Weathermen in New York and the mis-applied Florida bombing incident reported above. We have no intention of disputing the value of keeping any records whatsoever on known criminals. The question is -- and again none of the examples answer it -- whether the apprehension of these criminals was substantially aided by surveillance of activities which are legal, and moreover, whether any information was gained by such surveillance which could not have been obtained as readily by more conventional means.

The files are also justified on the basis of the necessity for preparedness to handle illegal or violent activities which might evolve from legal but potentially violent activities and demonstrations. According to General Johnson, former Chief of Staff of the Army, the army views itself as the last bulwark of defense of American Society. If it lo loses control, for example, of a Detroit-like riot, there is no higher force to which appeal may be made. This is h his justification for the Army's use of political surveillance. The same types of arguments, with lesser degrees of finality, are applied to operation by all state, local, and national law enforcement agencies.

It should be noted at this point, however, that high officials in the Justice Department have stated flatly that

most of the information gathered is useless for the purposes of prediction. To take an extreme example, consider the Army's attempt to apply counterinsurgency tactics developed for use in Southeast Asia to the Detroit riots of 1967. Such actions imply a basic misunderstanding of the issues and the players involved. A conspiracy to take (or re-take) a country is certainly different from a mindless riot.

The predictions of the Justice Department's intelligence files may also be subject to question. The Justice Department's Civil Disturbance Estimate of November 4, 1969 begins

> "It is my assessment that the potential for violence with resulting personal injuries and possible deaths, as well as damage to real and personal property, in connection with the demonstrations planned by the New Mobilization Committee...is extremely high. By extremely high I mean the liklihood of violence, its intensity, and extent, would be considerably beyond the violence which was witnessed during the Pentagon demonstration in October, 1967, the Democratic National Convention in Chicago in August, 1968, and the demonstrations in Chicago on October 14th conducted by the Students for a Democratic Society."

It is on the basis of such tremendously inaccurate predictions that policy decisions concerning government reaction to protest are made.

Another argument made for the harmlessness of data banks which are limited to recording of actions at public events is that such events are by definition public, which means that any actions performed there are meant to be known and are not private. However, Congressman Cornelius Gallagher has argued that a very dangerous problem in our society is the ability to make a man's past follow him around forever.

Speaking of the computer's ability to remember things forever, he has said:

> "Errors petrifying in a computerized record may be used to deny the adult an opportunity for which he is highly qualified....Society should not penalize the adult for his repented and redeemed sins as a child....
> "...we can program redemption out of American society...once you have paid the price for a mistake, you have the right to continue and develop your talents, free from a constant reminder that you have once faltered."
> (Gallagher, May 7, 1968)

Closely related to this is the last justification -- that "I have nothing to hide." If the discussion of the bases of privacy has not amply demonstrated the fallacy of this idea, consider Justice Goldberg's statement:

> "What is wrong with that? Simply this -- that everyone has something to hide; not something that he is necessarily ashamed of but that he wants for his own. That he once registered as a democrat, for example, or made an improvident investment, or engaged in a youthful escapade, not even criminal, or bought an Edsel. These are the sorts of facts that the state knows, but that we do not want it to know too well."

All of this should not be construed to imply that data files on political activities are inherently evil and should not be allowed. Rather, it should indicate that the arguments thusfar presented by the proponents of such files are inadequate at best. It is clear that society must be allowed some mechanisms by which to safeguard itself from violence. But it is important to realize that obtaining this protection requires certain tradeoffs, and that these tradeoffs must be explicitly considered at the time such mechanisms are constructed. It is abundantly clear, that such mechanisms for maintaining society's norms, if left to themselves, will

expand far beyond their intended function; if we are to maintain control of such institutions, we must closely regulate them from the very beginning.

As with any information system, the basic tradeoff to be considered is the extent to which individuals in a society choose to sacrifice their privacy rights in the interests of maintaining the norms of the society at large. It is clear that society has to protect itself against common criminals, lunatics, etc. It is our claim, however, that society can obtain the information it needs to protect itself from such people without infringing on the privacy rights of any except the usual known criminals and avowed subversive groups. To the extent that society enforces its norms through violations of the individual privacy rights of significant numbers of its citizens, the quality of life in that society is severely degraded, and its right to continued existence is subject to question.

B. Survey of Existing Data Banks

Retail credit bureau; Internal Revenue; F.B.I.; Dept. of Justice; Secret Service; H.E.W.; Housing and Urban Development; Customs Bureau; Civil Service; Navy; Air Force; C.I.A.; House of Representatives Internal Security Committee; Selective Service System; Dept. of Immigration and Naturalization; Dept. of State; State and local governments; New York Stock Exchange; Drinan.

PARTIAL SURVEY OF EXISTING DATA BANKS

This section will examine different data banks, presently in existance, in both the Federal and non-Federal sectors.

THE RETAIL CREDIT BUREAU

This nationwide company is number one in the retail credit investigation business. They have a total of 45 million reports on American citizens and issue copies of these reports together with newly created reports at the rate of 35 million per year. The price of the reports range from $5 to $25, depending on the quality of information the requesting organization desires. The Federal Government itself requested more than 10,000 reports on various individuals in 1967.

The company employs 6,300 trained inspectors, of whom approximately sixty percent have had some college education including about 1260 with Bachelor degrees.

The average report production is 11⅓ reports per day per inspector. These files are located in over 300 different locations throughout the United States.

Only about 5 percent of the reports are believed to contain unfavorable information. Furthermore, although an individual may discuss his report with the company, he may not examine its contents.

THE UNITED STATES INTERNAL REVENUE SERVICE

The I.R.S. has 15,000 employees including 1800 special investigative agents in the tax fraud division and has statutory authority for the collection of Federal tax revenues. In pursuit of this objective, the agents of the I.R.S. utilize a wide range of electronic equipment, a fact only recently available to the general public. Further, the I.R.S. refuses to divulge information about its agents and files, ostentatiously as a protection of privacy. Never the less, the Service will sell confidential tax return information on any United States tax payer, for $75 per reel of tape, to 23 other Federal agencies, to certain agencies of any of the states including the District of Columbia, and to over a dozen foreign countries. In addition, tax return information may be seen by the heads of a number of Federal agencies, some Congressional committees, the governors of every state, and by a Special Counsel to the President.

According to Senator Edward V. Long, writing in Playboy, the Treasury Department maintains a school in Washington, D.C. where agents are taught how to break and enter into buildings and install various electronic eavesdropping equipment.

Protection of tax information is presently a controversal subject. Although the I.R.S. states that information submitted on tax returns is confidential, some local

jurisdictions which had received tax data on individuals, according to the New York Times of June 28, 1970, were merely instructed to alert their employees that the unauthorized disclosure of Federal tax information was punishable by a $1000 fine. The I.R.S. apparently exerted no control over the use of the information.

THE FEDERAL BUREAU OF INVESTIGATION

The F.B.I. is authorized to collect data based on three seperate statutes. In 1940 President Roosevelt directed the Bureau to gather domestic intellegence information regarding subversive activities in the United States by organizations and individuals engaged in attempts to overthrow the Government. Second, the Federal Employee Security Program and the Internal Security Act of 1950 authorized the F.B.I. to gather information to be used by the Attorney General of the United States and by the Subversive Activities Control Board in the compilation of lists of subversive groups. Third, the F.B.I. is authorized to investigate all violations of Federal criminal laws including the Federal anti-riot law. The internal operations of the Bureau is under the direction of the Domestic Intellegence Division.

Each year eight million people are arrested in the U.S. and most police departments routinely send copies of the arrested person's fingerprints and arrest record to the Bureau. These files presently include the records of 50 million Americans who have, at some time, been arrested. The fingerprint

file alone is increasing at the rate of 30,000 files per day. Further, the local police often fail to inform the F.B.I. of the outcome of the arrest so that many files are still retained on persons who have been cleared of all charges.

The F.B.I. is currently proposing that its computerized National Crime Information Center (NCIC) intellegence center in Washington become a national crime information center to include all national information on individuals involved, in some way, with a criminal act and on whom there exists a file in some police department. The communication lines from this center would extend to all police agencies in the country.

The F.B.I. is also currently engaged in an argument with its parent agency-the Department of Justice. When the Justice Department established Project Search, a computerized national crime information system somewhat like the NCIC, the F.B.I. participated in the program as an observer. However, when the project's directors reported to the Department that any expanded system should include the right of an individual to examine his file, the F.B.I. subsequently advanced its own plans for a data bank after declaring that this proposal was unacceptable to the Bureau.

The F.B.I. has also recently been granted authority to release data on individuals to banks and insurance companies, according to Jared Stout in the October 11, 1970 issue of the Long Island Press.

The F.B.I.'s principal sources of domestic information

include publications generally available to the public, and state and local police files. Covert operations, such as wiretapping, are also engaged in. All of this data is usually kept in raw form with some reports going to other Federal agencies.

As a matter of interest, it should be noted that 50% more space in the new F.B.I. headquarters in Washington, D.C. has been allocated to domestic intelligence than to criminal and other intellegence operations.

THE DEPARTMENT OF JUSTICE

According to Jack Anderson, writing in the Washington Post of November 28, 1970, the Justice Department now has over 13,000 dossiers on anti-war demonstrators. Only a dozen or so could possibly be suspected of violating any law. Each week, the Justice Department issues computerized information about the potential disorders, region by region, throughout the United States, in four books each about two inches thick, and enclosed in brown cardboard covers. These report on the marches, rallies, organizations, and the individuals supporting them. Specific upcoming major events are also studied in the same way. It is interesting to note that no specific authorization was sought from Congress to set up the Justice Department computer files.

Since November 1969, when the Washington Moratorium events occurred, the Interdivisional Intelligence Unit of

the Department of Justice under the direction of James T. Devine, has supplanted the army's Counter-intelligence Analysis Division as the Federal Agency with authority for civil disturbance and related political intelligence operations. The unit maintains a computer system larger than the one formerly used by the army which was ordered to be shut down.

SECRET SERVICE

The Secret Service employs one of the newest and most sophisticated computers in the Federal Government. This computer functions to assist the Service in carrying out its extensive statutory authorithy which includes the following:

1. The collection of information pertaining to a threat or attempt by an individual, group or organization to harm or embarass anyone protected by the Secret Service or any high government official whether he is in the U.S. or abroad.

2. Information related to individuals, groups or organizations who have plotted, attempted, or carried out assassinations of high officials of this or a foreign government.

3. Information concerning the use of bodily harm as a political weapon including training used to carry out the act.

4. Information on persons who insist on personally contacting high government officials for the purpose of redress

of imaginary offenses.

5. Information on any person who makes written or oral statements about high government officials which are either threatening, irrational, or abusive.

6. Information on professional gate crashers.

7. Information on bombings.

8. Information on owners of firearms or other implements of war.

9. Information on all anti-American demonstrations in the U.S. and overseas and the collection of information on civil disturbances regardless of the cause for the disturbance.

DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE

HEW has a data bank containing the scholastic records, including teacher judgements, on over 300,000 children of migrant farm workers. There is presently no statutory authority over the distribution of this information.

The Social Security Administration maintains a large data bank containing information on every American who has ever received a Social Security number.

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

The Federal Housing Administration has a computerized data bank including the identities of 325,000 loan applicants. HUD also has its own adverse information file on groups and individuals and receives F.B.I. information on investigations of housing matters for addition to this file.

CUSTOMS BUREAU

The Customs Bureau has a computerized list of suspected or known smugglers which can be queried from a large number of boarder crossing points throughout the U.S. Since the system began in March of 1970 with 3000 initial entries, the file has grown over six times in size, and is continuing to grow. Known as the Custom Automated Data Processing Intellegence Network, the system is under scrutiny because it does not allow an individual to check the validity of the information in his file. CADPIN was designed to be fully compatible with other law enforcement computer systems when necessary. The information on the file is available to other Federal, state and local law enforcement agencies.

CIVIL SERVICE COMMISSION

The Commission maintains files on all current and former employees of the Federal Government and conducts investigations on all employment applicants. The Commission also maintains a subversive activities data bank containing the names of an estimated 1.5 million citizens. This is in addition to the employment files which contain over 10 million records.

DEPARTMENT OF THE NAVY

The Naval Intellegence Agencies maintain a large scale file on citizens who may represent a threat to naval installations, reportably including an intelligence file on political dissidents.

DEPARTMENT OF THE AIR FORCE

Like the Navy, the Air Force maintains files in support of its requirements for protecting air bases and other installations.

CENTRAL INTELLIGENCE AGENCY

The CIA has an extensive filing system on many Americans which is located at its Langley, Virginia headquarters.

U.S. HOUSE OF REPRESENTATIVES INTERNAL SECURITY COMMITTEE

The Committee maintains a list of radical campus speakers and had requested colleges to submit lists of speakers.

SELECTIVE SERVICE SYSTEM

A decentralized system of files on every American who has registered with the Selective Service System exists throughout the United States. A significant feature of these files is the right of an individual to inspect and add to his file at any time.

DEPARTMENT OF IMMIGRATION AND NATURALIZATION

The Department maintains a data bank containing information about all foreign nationals in the U.S.

U.S. DEPARTMENT OF STATE

The State Department's Passport Office retains files on

all Americans who apply for U.S. passports.

STATE AND LOCAL GOVERNMENTS

The State of Oklahoma maintains a secret agency directed by a former military officier which has the responsibility of collecting information on a large number of citizens and organizations. The agency is under the control of the Oklahoma National Guard. Individuals are not allowed to inspect their files nor has anyone's name ever been removed from the files.

The State of Pennsylvania is preparing to implement a five million dollar computer based information system with direct connection to the F.B.I.'s National Crime Information System in Washington. Most police organizations in the State will also be linked directly into the computer system. At present, the system is intended to contain information on criminal activities and motor registrations.

The New York City Police Department maintains a large file of unsubstantiated information about juveniles from which information has been given to welfare authorities, courts and schools.

The State of Massachusetts maintains a Subversive Activity Division in the State Office Building at Government Center in downtown Boston which retains files on peace, antiwar, and civil rights demonstrators. Up until April 1970, the information was available to colleges and universities seeking information

C. A case study of domestic intelligence:

the Army's Continental United States Intelligence Network.

The intelligence hierarchy; the Army's authority; early history of CONUS intelligence; collection methods; Blacklist and Compendium; status in 1969; usefulness of computer files; collection, processing, and dissemination; the outcry of 1970: movements toward reform; some observations.

INTRODUCTION

This section presents a detailed study of the Army's maintenance of intelligence files, especially personality files and blacklists, describing the lawful political activities of individuals and groups. Primary interest is focused on those files used for civil disturbance purposes, rather than on files used for security clearances and direct threats against Army property.

THE INTELLIGENCE HIERARCHY

There are two separate chains of command which maintain intelligence capabilities. The Intelligence Command (USAINTC) includes the Military Intelligence (MI) groups whose primary function is security clearance investigations. There are about 300 MI branch offices throughout the U.S., with 5 to 50 agents assigned to each branch office. These groups report directly to USAINTC headquarters at Fort Holabird, Maryland.

The second command includes the stateside G-2's of the Continental Army Command. These agents are trained to supply intelligence in combat situations. At one time, the MI groups were part of the G-2 units.

There is much duplication between these two groups. Both formerly collected civil disturbance information using similar methods and both passed this information on to the domestic intelligence section of the Counterintelligence Analysis Detachment (CIAD) of the Office of the Army Assistant Chief of Staff for Intelligence (OACSI).

THE ARMY'S AUTHORITY

Under the "inherent powers doctrine", some persons interpret Article 2 of the Constitution to imply that the President may engage in whatever "intelligence-gathering operations he believes are necessary to protect the security of the nation". However, others, including Christopher Pyle, a doctoral candidate in law at Columbia University, claim that this does not justify surveillance of lawful political activity. According to Pyle:

> "(this) would probably be forbidden by the Bill of Rights. The reason is the chilling effect which knowledge of surveillance has upon the willingness of citizens to exercise their freedoms of speech, press, and association, and their right to petition the government for redress of grievances...regardless of whether that effect was intended."
> (Pyle, "CONUS Intelligence: The Army Watches Civilian Politics.")

The courts have accepted this contention. For instance, in Anderson vs. Sills the New Jersey Superior Court declared most of that state's intelligence system unconstitutional because of a chilling effect.

Moreover, Pyle listed laws which "mark off the Army's responsibility for law enforcement from that of other agencies." He mentions several:

> "These include not only statutes which restrict the Army to a backup function in times of riot, but the laws which assign surveillance of unlawful political activity within the United States to the FBI and the Secret Service. Other sources of the Army's authority include the Uniform Code of Military Justice, which permits investigation of unlawful political activity within the armed services, and those laws and federal-state agreements under which the Army governs many of its installations."
> (Pyle, "CONUS Intelligence...")

The use of the Army as backup has decreased in frequency during the past two years by comparison to the riot-active years of 1967 and 1968.

SOME EARLY HISTORY OF CONUS INTELLIGENCE

The CONUS (Continental United States) Intelligence program began in the summer of 1965. It was supposed to provide an early warning system for civil disorders in which the Army might be required to intervene.

The year 1967 was marked by the Detroit and Newark riots, and the Peace March on the Pentagon. As a result of the events in Detroit, Cyrus Vance was appointed to head a commission to see what went wrong in Detroit. Among the conclusions of the commission was a recommendation for better intelligence. Several high officials in the Army thought that the computer could be used for the prediction of riots. Unfortunately, computer predictions are no better than the programmed procedure that humans use to instruct the computer. It is clear that the capabilities of computers were not at all understood by the people that decided to use them. Also in 1967 the Army widened its scope to include intelligence gathering on the political beliefs and activities of individuals and organizations active in the civil rights, white supremacy, black power, and anti-war movements.

In 1968, the riots after Martin Luther King's death resulted in the need for rapid movement of troops to Washington, Baltimore, and Chicago. Thus the "Domestic War Room" came into

existence as the Army prepared to fight in 25 cities simultaneously. The Domestic War Room included 200 men and a microfilm file including information from the FBI, state, and local officials. The files included packets on 150 urban areas, containing logistics information and, according to Pyle, information on individuals and groups such as the Young Americans for Freedom, the Southern Christian Leadership Conference, the Center for the Study of Democratic Institutions, Rear Admiral Arnold E. True and Brigadier General Hugh B. Hester (war critics), Georgia State Representative Julian Bond, and folk singers Joan Baez, Phil Ochs, and Arlo Guthrie. (Pyle, "CONUS Revisited..."). The Domestic War Room cost an estimated $2.7 million.

Another file that was created was a biographic file which could retrieve information on 4050 individuals, 500 of whom were not in the Army. This system was built using spare computer time by a lower-level officer who thought it would be useful. Officials at higher levels were unaware of the file's existence.

COLLECTION METHODS

Most of the information was obtained indirectly. There were many sources: newspapers and other media, local police, campus police, state police, FBI, Secret Service, and perhaps others. Overt observation was also used. Information collected in the field was usually reported by teletype to the U.S. Army Intelligence Command where the Director of

Investigations is responsible for storing the information and forwarding it to appropriate Department of Defense officials. An "agent report" will follow if the agent deems the incident of lasting value to the Army. Some former agents claim that performance is measured on the basis of volume and speed (sometimes implying the necessity for beating the Associated Press)) A military spokesman has denied this, claiming that an agent would have to justify a meaningless report to his branch leader. Consider, however, the following incident report:

> "PHILADELPHIA, PA: MEMBERS OF THE VIETNAM WEEK COMMITTEE COMPOSED LARGELY OF PROFESSORS AND STUDENTS OF THE UNIVERSITY OF PENNSYLVANIA, WILL CONDUCT A "SLEEP-IN" TO PROTEST THE SCHEDULED APPEARANCE OF DOW CHEMICAL COMPANY RECRUITERS ON CAMPUS. THE NEXT DAY, 19 MARCH, THE SAME ORGANIZATION WILL SPONSOR A PROTEST RALLY ON CAMPUS."
> (Pyle, CONUS INTELLIGENCE ...")

The relevance of this report to nation-wide planning for riot control is difficult to see.

Several examples of Army infiltration of civilian groups have been cited, including the Southern Christian Leadership Conference, the National Mobilization Committee, the Poor People's Campaign, and a Yippie commune on DuPont Circle during the Counterinaugural in 1969. Army agents posed as students at NYU, Columbia, City College of New York, and Fordham, were arrested at Howard University in Washington, D.C. for throwing rocks at police, posed as press photographers and newsmen, and pretended to be television reporters from the "Midwest News Service" interviewing demonstrators in Chicago, Washington, and Catonsville, Maryland.

The Army has even observed the Presidential Conventions. In Miami in 1968 the Army had agents on the convention floor. During the Democratic Convention in Chicago, according to Pyle, Army agents "posed as TV camera crews,...and two plainslothesmen from the staff of the Army Assistant Chief of Staff for Intelligence occupied assigned seats within the convention hall." This latter action occurred despite the CIAD's correct predictions that federal troops would not be needed.

The Army claims that all of these covert operations took place with the concurrence of the F.B.I.

In February 1969, Undersecretary McGiffert wrote a memo stating that his approval was required, in addition to that of the F.B.I., for any covert operations. The Army claims that no one has asked for this approval. There is indication that this policy is not being followed at lower levels, based on examples cited by former agents. For instance, according to Pyle, one of Oliver Peirce's assignments with the 5th MI detachment at Fort Carson, Colorado was:

> "To infiltrate a group called the Young Adults Church Project (YAP), which was established by a coalition of local church groups, the Young Democrats, and a ski club to operate a recreation center for emotionally disturbed young people. Although the project was entirely non-political, Peirce said, he and a soldier-informant were directed to make detailed reports on its meetings because one of the group's founders had attended anti-war demonstrations outside the fort and had once been a member of SDS." (Pyle, CONUS Revisited...)

A spokesman for the Army denies this, claiming that the former SDS'er had joined after the agent, that the agent

himself had gone to the commanding officer offering to report on this person, and that the commanding officer discouraged this reporting. The Army spokesman also disputed another of Pyle's charges -- that an informant was sent to the 1968 SDS National Convention in Boulder, Colorado. The spokesman claimed that two soldiers had been invited to attend the convention, that they did attend and were disappointed, and that they reported this.

Peirce also claimed that:

> "(the) 5th MID...assigned five undercover agents to monitor an anti-war vigil in the chapel of Colorado State College, maintained two full-time infiltrators within the local peace movement, and sent others to observe meetings of the Colorado Springs poverty board."
> (Pyle, CONUS Revisited...")

Moreover, Peirce claimed that these operations duplicated those of FBI, local, and state police, and the Colorado Springs office of the 113th MI group.

BLACKLIST AND COMPENDIUM

From May 14, 1968 to February 24, 1969 the Army published a blacklist, which they called an "identification list". This list, which contained mug shots and vital statistics on controversial citizens who the Army claimed had been active in past civil disturbances, was sent to 150 Army Intelligence and troop units, plus the F.B.I., the Justice Department, Naval and Air Force Intelligence, the C.I.A., and the U.S. embassies in West Germany and Canada. However, Pyle claimed that the Army "failed to mention that the list also contained

detailed descriptions of persons and organizations never involved in civil disturbances." (Pyle, CONUS Revisited...").

The Compendium was a two-volume loose-leaf encyclopedia termed the "Counterintelligence Research Project: Cities and Organizations of Interest and Individuals of Interest." The South Bend MI branch office prepared dossiers on individuals to go into the Compendium. These dossiers were 5x7 cards which included a picture of each person as well as his name, address, occupation, background, record of political groups with which he was affiliated, a list of political meetings, rallies, and demonstrations attended, and a summary of the subject's political views on various issues.

STATUS IN 1969

By 1969 the Army kept the following files of civil distrubance information:

1. Fort Holabird computer file, including a biographic file.
2. Microfilm archive in the Domestic War Room.
3. Blacklist and Compendium.
4. Continental Army Command computer file at Fort Monroe.
5. Local files maintained by MI branch offices (300 of them).
6. Local files maintained by stateside G-2's.

USEFULNESS OF COMPUTER FILES

Army officials have admitted that the information collected on civil disturbance was of little use in predicting civil

disturbance needs. As early as 1968 Undersecretary McGiffert wrote asking why the Army was collecting the information. Memos on this subject have been flowing from civilian leaders to military for the past two years, but there was no policy change before 1970.

These civil disturbances files did serve the curiosity of the Pentagon brass. Many generals called up regularly to obtain information on controversial personalities they saw on the news. One intelligence agent wrote an unclassified report of SDS chapters at four Pennsylvania colleges for a general and his daughter.

COLLECTION, PROCESSING, DISSEMINATION

There seems to have been little thought as to what information was collected. Collection decisions were made by the local agents. Due to the tremendous volume of information, there was probably little checking for accuracy, especially in the case of information obtained through liason with local officials.

Distribution of the information showed a similar lack of planning. Agents traded information with local officials and the F.B.I., although this was against Intelligence Command policy (one such incident occurred in the 113th MI group in 1969). The distribution of documents such as the Compendium included the Panama and European commands. The Compendium was also distributed to federal agencies such as the Civil Service Commission, the Secret Service, and the F.B.I. There was

no such thing as "need to know".

THE OUTCRY OF 1970: MOVEMENTS TOWARD REFORM

In January 1970 Christopher Pyle, a former Captain in Army intelligence, published an article entitled "CONUS Intelligence: the Army watches Civilian Politics" in the Washington Monthly. He also began to work closely with NBC ("First Tuesday", December 1, 1970), with WGBH in Boston ("The Advocates", October 27, 1970), and with the press. Pyle's first article described the CONUS Intelligence program and its dangers. Much of his information was obtained by debriefing former Army agents.

In the period immediately following the publishing of his first article, according to Pyle, the Pentagon's Office of Public Information refused comment. Also, Pyle claimed that "agents were forbidden to discuss any aspect of the program with newsmen and were warned that any who did would be prosecuted for breach of national security." (Pyle, "CONUS Revisited..."). The relevant files were classified to prevent public access to any information.

On the 22nd of January, Senator Ervin sent a letter to Stanley Resor, Secretary of the Army, concerning a "survey of the development and maintenance of databanks by Federal Departments and agencies." He went on to describe this study:

> "One of our purposes is to determine whether or not such data systems are being developed in accordance with constitutional standards of privacy and due process

> of law for the individual citizens involved. Another purpose is to help Congress ascertain the need for comprehensive legislation to govern all computerized databanks on individuals.
>
> "Our attention has been particularly directed to reports of the development and expansion of databanks at Fort Holabird, containing information on the personalities, on the political, economic and social beliefs and on the lawful community activities of American citizens.
>
> "To assist the Subcommittee in its study, we should appreciate your explaining to us: (1) the present situation concerning collection and storage of Army intelligence and other investigative data on private individuals, particularly at the Investigative Records Repository, but also at other data centers operated by the Army; and (2) future plans for expanding and further computerizing the present system."

Senator Ervin asked sixteen specific questions.

While Ervin received no answer at that time, the Army released a statement on January 26th. Pyle, in his second article, calls this statement

> "...the first in a series of partial admissions. In the jargon of the spy trade, such admissions are known as "plausible denials" because they are invested with just enough truth to mask an essential falsehood. Thus the Army confirmed the existence of the nationwide intelligence apparatus (true) but said it collected political intelligence only "in connection with Army civil disturbance responsibilities" (false). .."This is indident information only and does not include individual biographies or personality data" (false)." (Pyle, "CONUS Revisited)..")

Pyle also disputed Army claims with respect to infiltration and the blacklist.

Meanwhile, letters similar to Ervin's were sent to the Army by Congressman Gallagher and Senators Williams, Hart, Dole, Brooke, Percy, Fulbright, and Cook. Throughout the first part of February no response was made to these inquires. Congressman Gallagher became upset enough to threaten to hold hearings. The delay in an adequate response was in part due

to the fact that the Army's civilian hierarchy, which is supposed to supervise the military structure of the Army, was as surprised as the Congressmen when they learned the full extent of the situation from Pyle's first article. In the face of such pressures, Robert E. Jordan, General Counsel for the Army, determined to find out what was going on, and spoke to the Assistant Chief of Staff for Intelligence. He was particularly interested in the biographic file to which Pyle had referred. However, according to Pyle, the Assistant Chief of Staff "greatly downplayed the CONUS system's capabilities." It seems proper to assume that either he or the officers immediately under him knew about the biographic file. Jordan then went to Fort Holabird, where the existence of the biographic file was not disclosed (possibly due to confusion during the briefing). Finally, in mid-February, Jordan went to the computer operator, asked for a printout on Mrs. Martin Luther King, Jr., and watched as the computer printed a lengthy list of references to Mrs. King.

On the 25th of February, Jordan sent a form letter to the more than thirty Congressional inquiries, including Senator Ervin's letter of January 22. Each received the same letter regardless of the questions he had asked. Jordan first told of the Army's concern over Pyle's allegations because of the American tradition that separated the military from domestic politics. He minimized the Army's intelligence role in the civilian sector, and insisted that the Army has

long preferred to have civilian agencies meet these intelligence requirements. Jordan then went on to describe, in great detail, the Army's role in security clearance investigations (which was never at issue). Finally, in speaking about civil disturbance information, he insisted that the Army's legitimate concern did not include "minor forms of disturbances and lawful activities not likely to lead to major disturbances involving the use of federal resources." He claimed that the program has been under constant review, and that the widely distributed blacklist had been ordered destroyed. Furthermore, the Fort Holabird computer data bank "which included information about potential incidents and individuals involved in potential civil disturbance incidents" was destroyed because it did not help predict trends. He stated that "no computer databank of civil disturbance information is being maintained, and directives provide that no such system can be initiated without the approval of the Chief of Staff and the Secretary of the Army."

Mr. Jordan did not answer Senator Ervin's 16 specific questions from the January 22 letter. In particular, he failed to mention any other databanks containing investigative data on private individuals. However, Pyle, in his July article, listed several of these other databanks:

1. 375 copies of a two-volume loose-leaf encyclopedia on dissent compiled by CIAD (the Compendium).

2. Microfilm archives in the Domestic War Room. (Jordan did not find out about these until questioned by Congressman Gallagher).

3. Computerized databank on civil disturbances, political protests, and resistance in the Army (RITA) at the Continental Army Command HQ, Fort Monroe, Va.

4. Non-computerized regional databanks at each stateside Army command and at many military installations.

5. Non-computerized files at most of the Intelligence Command's 300 stateside intelligence group offices.

Congressman Gallagher seemed pleased with Jordan's response, though Pyle claimed he was aware sof the omissions. Ervin was not satisfied, and on the Senate floor on March 2, 1970, he stated that "while the Army's response is commendable, it raises more questions than it answers, and leaves a great many of the old questions unanswered." He wrote Secretary Resor on Febraary 27th requesting a complete report, especially with regard to civil disturbance databanks.

At about this time, according to Pyle, Congressman Gallagher received word regarding the reaction in the lower ranks of the Army to the public outcry:

> "On the morning after news reports about the dismantling of the CONUS system first appeared in the Washington papers...members of the 116th were... informed that their unit and its operations would be unaffected.... Files kept by the regional MI groups ...would remain intact...and members of the MI groups would continue their operations of surveillance, infiltration, and reporting as previously." (Pyle, "CONUS Revisited...")

In addition, Pyle mentioned that the 116th's files were classified to prevent their release. These files included a 5x7 card file on several thousand people in the Washington area.

Following Jordan's second surprise, this time with the

microfilm archive, the civilians in the Army began a concentrated effort to find out what was going on. On March 6, Secretary Resor sent a memorandum to the Chief of Staff of the Army requesting that he find out what computer systems existed. He repeated the Army policy toward such computerized systems as contained in Jordan's February 25th letter. On April 1, 1970, the Adjutant General, Kenneth G. Wickham, forwarded this request to the commanding generals. This letter, at one time classified, also requested a report on non-computerized information files related to activities, including civil disturbances, which involved civilians not affiliated with the Department of Defense. One computerized data bank was uncovered at Fort Hood, which the Army ordered destroyed after Fort Hood officials unsuccessfully attempted to justify it.

On March 20, 1970, Undersecretary of the Army Thaddeus Beal sent a long letter to Senator Ervin which he began by describing the security investigation program for uniformed members of the Army, civilian employees, and contractors' employees who worked on Army contracts. He reiterated the claim that no computer would be installed in the USAIRR, though the Defense Central Index of Investigations would be computerized. Beal also reiterated the Army policy toward computer databanks, first mentioned by Jordan, and stated that the Constitutional Rights Subcommittee would be informed whenever a computer databank was approved.

In describing the current policy toward the "spot report" system, Beal stated that information concerning outbreaks of

violence or incidents with a high potential for violence beyond the capability of state and local police and the National Guard to control" will be collected by liaison with other government agencies such as the F.B.I., reported by teletype to the Intelligence Command (not placed in a computer), and destroyed after 60 days.

Beal next described CIAD, which was established in OASCI to provide analysis such as civil disturbance estimates. The files, received from the F.B.I., are stored on microfilm, with a computerized index. CIAD is "closely supervised by OASCI and is not permitted to consider matters beyond its limited area of concern." CIAD at one time compiled and identification list with limited distribution to Army organizations with civil disturbance responsibilities.

Beal also wrote to Gallagher, claiming "the only other intelligence files concerning civilians maintained by the Army consist of the files maintained by the Counterintelligence Analysis Division." But, as Pyle pointed out in his second article,

> "No reference was made to: 1) the Continental Army Command's computer files at Fort Monroe, about which Gallagher had made specific inquiries; 2) the regional databanks kept by most of the 300 offices of the Army Intelligence Command; or 3) similar records maintained by the G-2's (intelligence officers) of each stateside Army command and of many Army posts."

Pyle also disputed Beal's description of CIAD's functions. In particular, he claimed the microfilm files existed to "satisfy the curiosity of the Pentagon's brass." Nor, says Pyle, did Beal mention the size of the microfilm

file (100,000 frames for worldwide intelligence information), or the card files on dissident individuals and groups. Moreover, Pyle mentioned several non-military organizations which received copies of the blacklist.

However, Beal's constraints on the Army were substantial, and Gallagher appeared satisfied.

During March, the ACLU brought suit against various high-ranking officials of the Army. The suit charged that the databanks and blacklists violated the Bill of Rights because of the effect which knowledge of such activities can have upon the willingness of citizens to exercise their freedoms of speech, press, association, and petition. The plaintiffs were 13 individuals and organizations whose non-violent, lawful politics had been the subject of widely distributed Army reports. The judge refused to hear testimony and dismissed the case, which is currently being appealed.

On June 9, Colonel Robert E. Lynch, acting Adjutant General, sent a policy statement to all commanding generals. It established "policy regarding the collection, reporting, processing, and storage of civil disturbance information." He mentioned reliance on the Justice Department for civil disturbance information needs. Lynch stated:

> "Under no circumstances will the Army acquire, report, process, or store civil disturbance information on civilian individuals or organizations whose activities cannot, in a reasonably direct manner, be related to a distinct threat of civil distrubance exceeding the law enforcement capabilites of local and state authorities, except as authorized in paragraphs 8 and 9d."

Paragraph 8 stated that "civil disturbance plans and supporting

materials will not include listings of organizations and personalities not affiliated with the Department of Defense", excluding, of course, local officials who have civil disturbance duties. Paragraph 9d stated that "after-action reports, where required for clarity, may contain names of individuals or organizations that were directly involved in the civil disturbance being reported. Inclusion of names of organizations and individuals will be kept to the absolute minimum for the purpose of the report."

Lynch also made several other policy statements. Army intelligence resources can only be used for collection of civil disturbance information when DCDPO "has made a determination that there is a distinct threat of civil disturbance beyond the capability of local and state officials to control." At these times, MI elements will maintain liason with appropriate local, state, and federal authorities, using other means of collection only on order of the Department of the Army, and will employ covert means only with concurrence of the F.B.I. and approval by the Undersecretary of the Army. CONARC can process civil disturbance information only when their troops are on standby status or are already assisting local officials. "Adverse civil disturbance information relating to persons or organizations...will not be stored except on order of the Department of the Army." Spot reports will be destroyed within 60 days and all other accumulated files, after a civil disturbance, will be destroyed or turned over to the Department of Justice. These policies did not cover "personnel security programs,

counterintelligence operations, and special collection requirements related to direct threats to Army personnel, installations, or material." Direct threats do not include anti-war protests and similar events. A copy of the complete letter is contained in the Appendix.

On July 29, 1970, Senator Ervin spoke out in Congress again, stating:

> "I am convinced that this public concern is caused by the failure of some agencies to limit their information activities to those reasonably necessary for administration of the laws they are charged by Congress with administering. It is also caused by the failure of responsible officials to inform the public and Congress honestly and squarely just why the information is needed, and what will be done with it, and it is caused by their frequent failure to assure due process to individuals who might be involved with the program or placed in a data bank."

He then went on to describe his correspondence with the Army. In addition to his interest in the constitutional issues, Ervin mentioned another reason for his interest:

> "the Army's data banks...appeared to be part of a vast network of intelligence-oriented systems which are being developed willy-nilly throughout our land, by government and by private industries. I believe that in these systems, where they contain the record of the individual's thoughts, beliefs, attitudes, habits, and personal activities, there may well rest a potential for political control and for intimidation which is alien to a society of free men."

Ervin also described letters he had written to Stanley Resor (July 27), to Melvin Laird (July 20), and to John Mitchell (June 9). Early in December, Robert Jordan answered the letter to Resor and part of the Laird letter. He mentioned an inspection program begun on July 13 to insure that the instructions specified in Lynch's letter are being carried out. Unfortunately, no new information was revealled in his letter,

and the answers to some questions, such as those relating to the specific subject areas concerning an individual's background, personal life, personality, and habits that are noted in each data bank were vague and incomplete. Jordan also mentioned that after the June 9 letter, the Army deleted all references to "essentially civil disturbance information" from the computerized index to the CIAD microfilm archive. According to another Army spokesman, the Lynch policy implied that CIAD should not answer unnecessary requests from curious generals.

The controversy flared again when Senator Ervin charged that the Army had spied on Senator Adlai Stevenson, former Governor Otto Kerner, and Representative Abner J. Mikva, all of Illinois. This charge was based on allegations made by James O'Brien, a former Army intelligence agent. The Army denied these charges, but apparently a dossier on Stevenson was kept in the files under "Operation Breadbasket".

On December 23rd, Defense Secretary Melvin Laird announced a reorganization of military intelligence operations to bring them under stricter civilian control and to ensure that they would be "completely consistent with constitutional rights, all other legal provisions, and national security needs." He also announced a sweeping review to take place by February 1, 1971. He said, "These activities must be conducted in a manner which recognizes and preserves individual human rights." According to Ervin's aides, these proclaimations may in fact have very little impact on the problem.

OBSERVATIONS

The Army has tried to deal with riots as conspiracies, citing the usefulness of blacklists in breaking up guerilla organizations in Southeast Asia. The National Advisory Commission on Civil Disorders found such analysis worthless in evaluating ghetto riots.

In fact, at the height of the Detroit riots, General Yarborough instructed his staff in the Domestic War Room: "Men, get out your counterinsurgency manuals. We have an insurgency on our hands." As one officer later observed, "There we were plotting power plants, radio stations, and armories when we should have been locating the liquor and color-television stores instead." (Pyle, "CONUS Intelligence...").

Even though the intelligence network was ineffective and unjustified, the Army bureaucracy worked very slowly to significantly reduce the domestic intelligence program. In fact, two years of letters between the civilian and military leaders produced no changes. Reductions in the programs were undertaken only in the face of severe Congressional pressure triggered by Pyle's articles. As Pyle said: "Without the threat of hearings, the Army's civilian leaders are not likely to end their evasions and deceptions, admit the full scope of the program, or reconsider its needs or consequences. They are the crisis managers of their bureaucracy. Threats, not suggestions, determine their agenda." With no crisis to force an overall evaluation of the domestic intelligence program, collection of data became a goal in itself as individual

members of the bureaucracy toiled to build their own small empires through always having enough data to answer any question which came down from above.

Simply issuing a directive is an empty gesture. In order to be effective, such directives must be communicated, understood, and followed. There have been several instances where Army directives have suffered lengthy communications delays, and where orders that were properly delivered were misunderstood. Moreover, instances of conscious concealment of facts from higher officers have been alleged. It might not be too surprising to discover that the present strict policies are not being strictly enforced. To take one example, former agent Edward Sohier reports that when the CIAD received the order to destroy the Compendium, they first archived all of the information on microfilm.

It appears that temporary military men -- the "in-and-outers" -- who were willing to speak out against Army policies were responsible for whatever changes have been made to date. Both Pyle and the agents he interviewed were temporary men. The structure of the military establishment is such that the incentive for career officers is not to rock the boat. Such changes as we have seen would in all likelihood not occur in an all-volunteer Army. Moreover, there appears to be even less incentive for change in the Justice Department System.

The Army may be misusing the classification system, in violation of the Freedom of Information Act. For example, Wickham's letter of April 1 was classified on no justifiable

basis, as were the files of the 116th MI mentioned above.

The military high command, the civilian hierarchy, and the authors of this report all experienced considerable difficulties in discovering the actual facts. According to Schier,

> "A lot of intelligence people felt no responsibility to tell the truth to anybody outside the intelligence community"
> (Sunday Herald Traveler, Sec. 3, page 15, Jan.3,1971 Boston)

including the Army general counsel. Schier claimed that one team of which he was a member lied outright to Jordan about the microfilm files.

Moreover, many military officials are very difficult to interview. Although we were received graciously, they volunteered little information, and only answered the questions they were asked. Therefore, an interviewer who goes armed with insufficient facts is unlikely to uncover the important aspects of the situation. In addition, potentially embarassing questions are frequently met with categorical denials, which upon more specific questioning are retracted.

We found the civilian hierarchy much more open during an interview.

D. Potential Future Problems

In his first article, Pyle dealt with the dangers inherent in the domestic intelligence community:

> "...it is not enough to reform the Army. The Intelligence Command is only one member of a huge, informal community of domestic intelligence agencies. Other members of the community include not only the FBI, the Secret Service, the Air Force, and the Navy, but hundreds of state and municipal police departments. Some of the latter are surprisingly large. The New York City Police Department's Bureau of Special Services, for example, employs over 120 agents and has an annual budget in excess of $1 million.
>
> "Each of these organizations now shares with the Army the capability to inhibit people in the exercise of their rights, even without trying. By collaborating, they could become a potent political force in their own right. Thus as the Army, the FBI, and the Justice Department strive to coordinate these agencies through the establishment of wire services, hot lines, and computerized data banks, it is essential that the American public and its representatives be equally energetic in the imposition of checks and balances. In particular, special efforts should be made to prevent needless concentrations of information. The United States may be able to survive the centralization of intelligence files without becoming totalitarian, but it most certainly cannot become totalitarian without centralized intelligence files. The checks must be designed with the most unscrupulous of administrators in mind. The fact that we may trust the current heads of our investigative agencies is no guarantee that these agencies will not one day come under the control of men for whom the investigatory power is a weapon to be wielded against political and personal foes."

It is not possible sto over-emphasize the volume and complexity of the problems related to access control and quality of data that arise as data banks and communications systems are interfaced. Validation of sensitive data obtained through a nation-wide conglomeration of systems such as are evolving in America would be a nearly impossible task.

But even successful prevention of such interfacing will not solve the problem. The rather complete lack of incentives

for system builders to provide privacy controls, coupled with a lack of understanding of the meaning of privacy cause systems to tend towards being worse instead of better. One system which should be watched carefully is that maintained by the Justice Department, which has no "in-and-outers" to serve as its conscience, and which has taken over the duties which Army intelligence has recently dropped.

PART IV: CONCLUSIONS AND RECOMMENDATIONS FOR THE FUTURE

A. Conclusions

JUSTIFICATION FOR CONCERN

1. There is a widespread public ignorance of the effect of everyday actions upon individual privacy.

2. In spite of substantial concern over the invasions of privacy expressed by all branches of government, by the private sector, and by the media, the mechanisms for privacy protection in America are very few and very weak.

WHAT IS PRIVACY

1. There is no comprehensive definition of privacy which is widely accepted; however, at least one excellent definition exists:

> "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others....The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process...in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms."
> (Westin, A., Privacy and Freedom)

2. Privacy serves four essential functions: it provides personal autonomy; it provides emotional release; it allows self-evaluation and introspection; and it allows for controlled transfer of information.

3. Much evidence exists that privacy is a biological necessity for homo sapiens.

4. The privacy decision is a tradeoff between the individual's desire to be, in fact, individual, and his desire to partake in society. Society places constraints on this

decision through its various institutions.

PRIVACY AND THE LAW

1. Privacy was not explicitly mentioned in the Constitution because it was much less a problem than it is now. If the Constitution is read in the context of the time in which it was written, then it is clear that the writers protected privacy in every way they knew how.
2. The Supreme Court has recognized a right to privacy as being implicit in a free society, but their definition of "privacy" has been very narrow indeed.
3. A number of Constitutional bases for the right to privacy exist in the 1st, 4th, 5th, and 14th Amendments, but the interpretation by the courts has varied from case to case.
4. Many technical barriers inherent in the legal system make it difficult, if not impossible, for a private citizen to bring suit and win on the grounds of invasion of privacy, especially if the suit is against the government.
5. Advancing technology, particularly in terms of high speed information processing devices, is rapidly destroying whatever competence the courts had in dealing with privacy issues.
6. The doctrine of the Chilling Effect on civil liberties has basis in law going back to 1947. Again, interpretation by the courts has varied.

HOW PRIVACY IS INVADED

1. Methodology for invading privacy ranges from simply asking questions to search of available public records to complete physical and psychological surveillance.

PRIVACY AND TECHNOLOGY

1. A very well-developed market exists for a wide range of increasingly effective devices for covert collection of data. The buyers include numerous government agencies as well as uncountable private firms.
2. A market for counter-espionage devices exists, but it is much less well-developed.
3. Industrial espionage causes losses of at least three billion dollars per year.
4. The computer is an amoral implement -- it serves only to amplify man's ability to process data for good or evil purposes. The magnitude of that amplification is extremely great.
5. A large variety of technical solutions to access control and security issues related to computerized information exist. These are not widely implemented due to a combination of high (not excessive) cost, low incentive on the part of system designers to consider privacy issues, and a general lack of sophistication on the part of government and industry system builders and of computer manufacturers.
6. Although not all of the technical difficulties have been overcome, the primary problems with computers are human

in nature, and should be the primary focus of our attention.

AN INITIAL SOLUTION AND ITS SHORTCOMINGS

1. The most commonly proposed solution to privacy problems -- to let an individual see and correct his own file -- is oversimplistic on several counts: it 1) does not take account of groups whose privacy is invaded, 2) assumes the individual is qualified to correct his own record, and 3) does not account for conflicts of privacy.
2. A first cut at a solution could be to distinguish between objectively provable fact and opinions and unverified data.

THE CASE IN FAVOR OF DATA BANKS

1. Collection of data is necessary for the existence of society. Three main forces driving man to collect and disseminate data are 1) the management functions of a complex society, 2) the resolution of conflicts of individual rights, and 3) the value inherent in dissemination of knowledge. Major problems arise when information collected for one of these three purposes is disseminated for another.

CRITERIA FOR EVALUATION OF INDIVIDUAL DATA BANKS

1. The dimensions for evaluation are 1) the criteria for being included as input, 2) the procedures for quality

control of data, 3) the methodology for processing raw data to get useful information, 4) access control of output information, and 5) the social effects of the system. The social costs must be traded off against the social benefits.

JUSTIFICATION GIVEN FOR POLITICAL INTELLIGENCE FILES

1. Reasons given for the existence of current files are 1) their deterrent power, 2) aid in apprehension of criminals, 3) the necessity for preparedness to handle violent activities, 4) the public nature of the actions involved, and 5) the assumption that honest people have nothing to hide.
2. These arguments are inadequate.

SURVEY OF EXISTING DATA BANKS

1. A very large number of local, state, federal, and private agencies are currently in the business of collecting data on citizens. The vast majority of such operations are legitimate. Some are illegitimate. Almost all suffer from important deficiencies in one or more of the evaluation criteria.

THE ARMY'S CONUS INTELLIGENCE NETWORK

1. Army leaders have admitted that much of the civil disturbance information system was useless in that it did not help to predict trends for use of federal troops in civil disturbances.

2. The Army has issued orders to severely cut back civil disturbance information collectinn, processing, reporting, and storage. They now rely on the JJustice Department for much of this information.
3. The most objectionable file was the computerized biographic file which was created probably without the knowledge of top military and civilian officials.
4. Collection methods included liason with local, state, and federal authorities, overt observation, and covert observation. The covert observation and infiltration, was against official Army policy.
5. Civilian officials had a great deal of trouble discovering the extent of CONUS Intelligence from their military subordinates.
6. Letters from the Army to Congress were often incomplete, and, in some instances, contained falsehoods.
7. The Army tried to deal with riots as conspiracies.
8. The civilian leadership of the Army worked quickly to limit CONUS intelligence only under severe Congressional pressure caused by Pyle's articles. In the previous two years, the program had been under review, but not action had been taken. The civilian leaders' agendas are determined by threats, not by suggestions.
9. CONUS Intelligence served the curiosity of Pentagon officials.
10. Army orders are not always communicated, understood, or followed. Thus it is possible that their present strict policies are not being carried out.

11. Temporary military men were responsible for the changes to date.

12. The Army used the classification system to prevent embarrassment.

13. Military personnel are gracious but not helpful to investigators of this problem. The civilian hierarchy is much more open.

POTENTIAL FUTURE PROBLEMS

1. Concentration on the Army's problems has obscured the many other data bases at all levels of government and industry which are equally deserving of attention.

2. Prevention of the integration of the data bases which form the intelligence network is highly desirable, since problems with access control and data quality are very much much more severe in such integrated networks.

3. In addition, careful scrutiny must be given to individual data bases, since the tendency is for them to go from bad to worse if left alone.

B. Recommendations for the future

We feel that it is extremely important to deal now with the domestic intelligence community because there is presently no motivation for system builders to protect the rights of American citizens, and because the social costs of the systems which are evolving is so great. However, these recommendations may be applied to any data bank, either manual or computerized.

First, a comprehensive national policy is needed. This policy should approve of a data bank only if it serves a legitimate need of a legitimate organization -- that is, if the data bank can be directly related to one of the three forces for data collection. What is needed is a conscious weighing of the social costs vs. the social benefits. In the case of the Army, Pyle has said that we must

> "define the Army's authority to monitor civilian politics in light of such principles as civilian control of the military, state and civilian primacy in law enforcement, compartmentalization and decentralization of intelligence duties, and obedience to the Constitutional scheme of separate branches of government sharing policy-making powers."

The philosophy of the cost/benefit analysis should be "guilty until proven innocent." There are at least three types of social costs -- 1) direct cost in resources expended by the organization; 2) indirect cost due to the Chilling Effect and the erosion of civil liberties; and 3) cost due to the possibility of misuse by unscrupulous administrators. Six issues must be considered in evaluating social costs -- 1) the criteria for being included as input; 2) quality control of input data; 3) processing procedures; 4) access control of

output information; 5) the degree of centralization; and 6) interfaces with other systems.

In terms of benefits, the system should be related in a very direct manner to one of the three forces for data collection -- 1) to serve the management function; 2) to aid in resolving conflicts of individual rights; or 3) to disseminate knowledge for its own sake. However, it is also important not to hinder unnecessarily any institution in its efforts to legitimately perform one of these functions.

We feel that such a policy could be stated as law.

Second, a means to enforce this policy is needed. Enforcement must be carried to the lowest levels of affected organizations. Furthermore, it is clear that present legal means for dealing with existing (and future) data banks are inadequate and must be improved so that it is possible to show "invasion of privacy" in time to do something about it. Preventive measures are needed due to the irreversible nature of violations of privacy.

One way to implement this control might be a civilian advisory board serving the same function for data banks that Certified Public Accountants perform for company ledgers. Careful consideration should be given to Senator Ervin's proposal to

> "create a Federal agency with powers to register all data bank operations, military and civilian, to demand justification for the records kept and to enforce a citizen's right to examine and to challenge data which could haunt his reputation, even his ability to earn a livelihood, for the rest of his days."
> (N.Y. Times, 12/27/70)

However, legislative and judicial action at all levels is not enough; individual citizens must be made cognizant of the issues and solutions that this report raises for consideration. True, system builders must be educated in the variety of technical considerations for protection of privacy and given incentives to use them. Incentives for further research should also be provided. But the job of protecting our privacy lies neither with the systems programmer nor with the computer manufacturer; it lies with us. Only by increasing the sophistication of each citizen in matters regarding his relationship to the society in which he lives can we prevent "freedom" from becoming an empty word in America.

APPENDIX

DEPARTMENT OF THE ARMY
OFFICE OF THE ADJUTANT GENERAL
WASHINGTON, D.C. 20310

IN REPLY REFER TO

AGDA (M) (25 May 70) ACSI-CICD 9 June 1970

SUBJECT: Collection, Reporting, Processing, and Storage of Civil Disturbance Information

SEE DISTRIBUTION

1. PURPOSE. This letter establishes Department of the Army policy regarding the collection, reporting, processing, and storage of civil disturbance information. It is applicable within the Continental United States, the States of Alaska and Hawaii, and Puerto Rico. It applies to all Army commands within those geographic areas.

2. DEFINITIONS.

a. Civil disturbance -- A situation in which a civil jurisdiction is required to apply a greater than usual degree of police enforcement in order to insure the maintenance of law and order.

b. Civil jurisdiction -- A town, city, county, or State; a legal corporate government within the Continental United States, Alaska, Hawaii, or Puerto Rico other than the Federal Government or its departments and agencies.

c. Collection -- For purposes of this policy, the acquisition of information in any manner, to include direct observation, liaison with official agencies, or solicitation from official or unofficial sources.

d. Law and order -- A condition in which a reasonable degree of the normal operations of a civil jurisdiction is possible.

e. Police enforcement -- That force available to a civil jurisdiction in order to insure law and order, such as a city police department, a county sheriff's office, State police, or National Guard in State service.

f. Processing -- The collation, evaluation, and analysis of raw information in order to produce finished intelligence.

g. Reporting -- For purposes of this policy, communicating information to another person or organization, whether orally, mechanically, or electrically.

AGDA (M) (25 May 70) ACSI-CICD 9 June 1970

SUBJECT: Collection, Reporting, Processing, and Storage of Civil Disturbance Information

h. Storage -- For purposes of this policy, the retention of information in any way, to include card files, dossiers, folders, computers, or punch cards.

3. GENERAL.

a. Public order is the responsibility of local and State governments and Federal civilian agencies. The Attorney General is the chief Executive Branch officer responsible for coordination of all Federal Government activities related to civil disturbances. Military forces are responsible for action only when the President has determined, in accordance with Chapter 15, Title 10, U.S. Code, that the situation is beyond the capability of civilian agencies to control.

b. The investigative jurisdiction of the Army with regard to espionage, sabotage, and subversion is in accordance with Executive Order 10450, dated 27 April 1953. It is delineated in AR 381-115, 2 July 1969, and is limited to:

(1) The investigation and disposal of all cases in these categories involving active and retired military personnel of the Army.

(2) The investigation and disposal of all cases in these categories of civilian employees of the Army outside the United States and its possessions.

(3) The disposal of cases on civilian employees of the Army inside the United States and its possessions.

c. The Department of the Army relies upon the Department of Justice at the national level to furnish civil disturbance threat information required to support planning throughout the Army for military civil disturbance needs.

d. The Department of the Army relies upon the Department of Justice at the national level to furnish early warning of civil disturbance situations which may exceed the capabilities for control by local and State authorities.

e. Under no circumstances will the Army acquire, report, process, or store civil disturbance information on civilian individuals or organizations whose activities cannot, in a reasonably direct manner, be related to a distinct threat of civil disturbance exceeding the law enforcement capabilities of local and State authorities, except as authorized in paragraphs 8 and 9d.

AGDA (M) (25 May 70) ACSI-CICD 9 June 1970

SUBJECT: Collection, Reporting, Processing, and Storage of Civil Disturbance Information

4. COLLECTION.

a. Army intelligence resources will not be used for the collection of civil disturbance information until the Director for Civil Disturbance Planning and Operations, or the Commander in Chief, Atlantic (CINCLANT) in the case of Puerto Rico only, has made a determination that there is a distinct threat of civil disturbance beyond the capability of local and State authorities to control.

b. Army Military Intelligence elements possessing counterintelligence resources will maintain the capability to collect civil disturbance threat information during a period in which there is a distinct threat of, or actual, civil disturbance requiring the use of Federal military forces.

c. Within the District of Columbia, the criterion is a distinct threat of civil disturbance beyond the capability of the Metropolitan Police to control.

d. Civil disturbance information collection capability of Army elements in the Continental United States, Alaska, or Hawaii will not be employed except on Department of the Army order or, in the case of Puerto Rico, on order of CINCLANT.

e. On activation by the Department of the Army, or CINCLANT for Puerto Rico, Military Intelligence elements possessing counterintelligence capability will:

(1) Establish and maintain liaison with appropriate local, State, and Federal authorities.

(2) Through liaison, collect civil disturbance information concerning incidents, general situation, and estimate of civil authorities as to their continued capability to control the situation.

(3) Report collection results to Department of the Army, ATTN: ACSI-IA, and DCDPO. In Puerto Rico only, report results to CINCLANT with information copies to DA, ATTN: ACSI-IA, and DCDPO.

(4) Keep appropriate commanders informed.

(5) Provide intelligence support to the Personal Liaison Officer, Chief of Staff, Army, and the Task Force Commander on arrival in the affected area.

(6) Recommend methods of overt collection, other than liaison, if required, to Department of the Army for approval.

AGDA (M) (25 May 70) ACSI-CICD 9 June 1970

SUBJECT: Collection, Reporting, Processing, and Storage of Civil Disturbance Information

f. Army Military Intelligence elements will employ methods of collection other than liaison only on order of Department of the Army.

g. Covert agent operations will not be used to obtain civil disturbance information on individuals or organizations without the concurrence of the Federal Bureau of Investigation and the specific approval of each operation by the Under Secretary of the Army.

h. Unsolicited Sources.

(1) So-called walk-in sources who volunteer civil disturbance information to Army elements will be referred to appropriate local police or local offices of the Federal Bureau of Investigation. If the source refuses such referral the information will be obtained and immediately furnished to the proper office.

(2) Information received from anonymous telephone callers or written messages will be referred as indicated in paragraph 4h(1) above.

5. REPORTING.

a. Army elements will maintain the capability of reporting civil disturbance information.

b. Civil disturbance information reporting will be activated only on Department of the Army order. In Puerto Rico, reporting will be activated only on order of CINCLANT.

6. PROCESSING.

a. OACSI, DA, has the sole responsibility for processing civil disturbance information in accordance with the definition outlined in paragraph 2 above at all times when Federal troops are not actually placed on standby or committed.

b. When the Director of Civil Disturbance Planning and Operations directs that Federal troops be placed on standby or committed to assist in restoring order, those Army elements involved will also be responsible for processing civil disturbance information in support of their local planning.

7. DISSEMINATION. Analyzed reports will be furnished to appropriate major Army commands in CONUS, Alaska, Hawaii, and Puerto Rico, when it appears that a civil disturbance poses a distinct threat beyond the capabilities of local and State authorities to control.

AGDA (M) (25 May 70) ACSI-CICD 9 June 1970

SUBJECT: Collection, Reporting, Processing, and Storage of Civil Disturbance Information

8. PLANNING. Civil disturbance plans and supporting materials will not include listings of organizations and personalities not affiliated with the Department of Defense. Exceptions to this policy are:

a. Listings of local, State, and Federal officials whose duties include responsibilities related to control of civil disturbances may be compiled and maintained.

b. Appropriate data on vital public and commercial installations/facilities or private businesses and facilities which are attractive targets for persons or groups engaged in civil disorder may be compiled and maintained.

9. STORAGE.

a. Army elements will be prepared to store civil disturbance information during a period in which there is a distinct threat of, or an actual, civil disturbance requiring the use of Federal military forces.

b. Adverse civil disturbance information relating to persons or organizations within the Continental United States, Alaska, Hawaii, or Puerto Rico, will not be stored except on order of Department of the Army.

c. Spot reports generated by activation of civil disturbance information collection will be destroyed within 60 days of the termination of the situation to which they refer.

d. After-action reports,where required for clarity, may contain names of individuals or organizations that were directly involved in the civil disturbance being reported. Inclusion of names of organizations and individuals will be kept to the absolute minimum for the purpose of the report.

e. Upon termination of a civil disturbance situation, the nature and extent of all accumulated files other than spot reports and after-action reports will be reported to Department of the Army, ATTN: ACSI-CIC, with recommendation for destruction or release to the Department of Justice.

f. Army elements will be prepared, on Department of the Army order, to destroy accumulated files or forward them to Department of the Army, ATTN: ACSI-CIC, for release to Department of Justice.

g. Computerized data banks for storage of civil disturbance information will not be instituted or retained without the approval of the Chief of Staff and the Secretary of the Army.

AGDA (M) (25 May 70) ACSI-CICD 9 June 1970

SUBJECT: Collection, Reporting, Processing, and Storage of Civil Disturbance Information

10. The collection, reporting, processing, and storage of information related to Army personnel security programs, counterintelligence operations, and special collection requirements related to direct threats to Army personnel, installations, or materiel are not affected by this letter.

BY ORDER OF THE SECRETARY OF THE ARMY:

ROBERT E. LYNCH
Colonel, AGC
Acting The Adjutant General

DISTRIBUTION:
Commander in Chief, US Army, Pacific
Commanding Generals:
US Continental Army Command
CONUS Armies and Military District of Washington
US Army Materiel Command
US Army Combat Developments Command
US Army Strategic Communications Command
US Army Security Agency
US Army Air Defense Command
US Army Intelligence Command
US Army SAFEGUARD System Command
US Army Computer Systems Command
US Army, Alaska

Copies Furnished:
Commander in Chief, US Army, Europe
Commander in Chief, Atlantic
Commander, US Army Forces Southern Command

BIBLIOGRAPHIES

GENERAL BIBLIOGRAPHY

Brown, Robert M., The Electronic Invasion. John F. Rider Publisher, Inc., New York, 1967.

Carnegie Quarterly, "Our Not So Private Lives: Surveillance and Freedom". Carnegie Corporation of New York. Volume XV, Number 2, Spring 1967. New York.

David, E. E. and R. M. Fano, "Some Thoughts About the Social Implications of Accessible Computing". Proceedings-Fall Joint Computer Conference, 1965.

Ervin Jr., Sam J., "The Computer and Individual Privacy". Remarks in the Congressional Record, Volume 113, Number 37, March 8, 1967. Washington.

_____ "Privacy, The Census, and Federal Questionnaires". Remarks in the Congressional Record, Volume 115, Number 108, June 30, 1969. Washington.

_____ "Computers and Individual Privacy". Remarks in the Congressional Record, Volume 115, Number 184, November 10, 1969. Washington.

Fano, Robert M., "Implications of Computers to Society". Paper presented at the Kiewit Computation Center Dedication and Conference, Dartmouth College, Hanover, New Hampshire, December 2-3, 1966.

_____ "Computers in Human Society-For Good or Ill?". Technology Review, Volume 72, Number 5, March 1970, Massachusetts Institute of Technology, Cambridge.

_____ "The Computer Utility and the Community". 1967 IEEE International Convention Record, volume 15, session 52.
New York City.

Fosburgh, Lacey, "23 to Study Computer Threat". Article in the New York Times, Thursday, March 12, 1970. New York.

Gallagher, Cornelius E., "Technology and Society: A Conflict of Interest?". Remarks in the Congressional Record, Volume 115, Number 55, April 1, 1969. Washington.

_____ "Personal Privacy, Data Security, and a Free America". Remarks in the Congressional Record, September 23, 1970. Washington.

_____ "Science, Privacy, and Law-The Need for a Balance". Remarks in the Congressional Record, August 18, 1966. Washington.

_____ Speech before the American Management Association, March 8, 1968, New York.

_____ Speech before the Ninth Practicum on Practical Politics, May 7, 1968, Jersey City State College, New Jersey.

Ruggles, Richard, "How a Data Bank Might Operate". Think, Volume 35, Number 3, May-June 1969, Armonk, New York.

Sprague, Richard E., "The Invasion of Privacy and a National Information Utility for Individuals". Computers and Automation, January, 1970.

Stone, M. G. and Warner, Malcolm, "Politics, Privacy, and Computers".

Westin, Alan F., Privacy and Freedom. New York, Atheneum, 1967.

_____ "Life, Liberty and the Pursuit of Privacy". Think, Volume 35, Number 3, May-June 1969. Armonk, New York.

_____ "Computers and the Protection of Privacy". Technology Review, Volume 71, Number 6, April 1969. Massachusetts Institute of Technology, Cambridge.

BIBLIOGRAPHY: LEGAL ASPECTS

"Anderson vs. Sills," Harvard Law Review, Vol. 83/4, February, 1970.

"Chilling Effect in Constitutional Law," Columbia Law Review, Vol. 69/5, May, 1969.

Congressional Record, Senate, July 29, 1970.

"Harvard Civil Rights,' Civil Liberties Law Review, Vol. 5/1, January, 1970.

Miller, Arthur R., "Personal Privacy in Computer Age;" Michigan Law Review, Vol. 67/6, April, 1969.

Reich, Charles A., Professor, Yale, Law School, Statement of, "Committee on the Computer and Invasion of Privacy," Congressman Gallagher, 1966.

"Tatum, Arlo, vs. Melvin Laird, Brief for Appelants," United States Court of Appeals, District of Columbia Circuit, No. 24.203.

BIBLIOGRAPHY: SURVEY OF DATA BANKS

Anderson, Jack, The Washington Post, November 28, 1970. Washington.

Bride, Edward J., "'Clean' System Could Lead Way in Law Enforcement". Computerworld, August 26, 1970.

Congress, U.S., "Retail Credit Corporation of Alanta, Georgia". Hearings before a Subcommittee of the Committee on Government Operations of the House of Representatives. Ninetieth Congress, Second Session, May 16, 1968. U.S. Government Printing Office, Washington, 1969.

_____ "Privacy and the National Data Bank Concept". Thirty-fifth Report by the Committee on Government Operations of the House of Representatives, August 2, 1968. U.S. Government Printing Office, Washington, 1968.

Data Systems News, "Privacy and the Computer". August-September, 1970.

Delaney, Paul, "New Security Watcher". New York Times, November 13, 1970, New York.

Ervin, Jr., Sam J., "Announcement of Hearings: Federal Data Banks and the Bill of Rights". Congressional Record, Volume 116, Number 155, September 8, 1970. Washington.

_____ "Secret Service Guidelines: Protection of the President and Protection of Individual Rights". Congressional Record, Volume 115, Number 208, December 15, 1969. Washington.

Flanagan, Mike, "Secret Bartlett Agency 'Watching' Sooners". Tulsa Daily World, Tulsa, Oklahoma, July 11, 1970.

Franklin, Ben A., "Federal Computers Amass Files on Suspect Citizens". New York Times, June 28, 1970. New York.

Goldhaber, Samuel Z., "Joe McCarthy Legacy is Still Alive in Massachusetts". Harvard Summer News, Friday, July 18, 1969.

Graham, Fred P., "Mitchell to Seek Subversion Curbs". New York Times, November 13, 1970. New York.

_____ "F.B.I.: When Should Its Arrest Records Be Expunged?". New York Times, n.d., New York.

_____, "President to Get Program to Curb Terror Bombings". New York Times, October 31, 1970. New York.

Kondracke, Morton, "Army Has Closed Down Political Computer, but Justice Department Maintains Bigger One". Chicago Sun-Times, March 9, 1970. Chicago Illinois.

Lang, John S., Big Brother (U.S.) Is Watching You". Sunday Herald Traveler, April 19, 1970. Boston, Massachusetts.

Library of Congress, Legislative Reference Service, "The Federal Data Center: Proposals and Reactions". June 14, 1968. Washington, D.C.

Long, Edward V., "Big Brother in America". Playboy. n.d.

Marshall, Eliot, "I Spy, You Spy". The New Republic, October 3, 1970.

Oelsner, Lesley, "Suit Challenges Data on Youths". New York Times, August 9, 1970. New York.

Ricki, Damon, "Vestiges of Joe McCarthy". Boston After Dark, May 26, 1970. Boston, Massachusetts.

Senate Subcommittee on Constitutional Rights, U.S., "Ervin Releases Census-Privacy-Computer Report; Notes HEW Concern on Privacy and Social Security Numbers". October 20, 1970. Washington, D.C.

Stout, Jared, "FBI vs. State Agencies". Long Island Press, October 11, 1970. Long Island, New York.

_____, "Computers Being Armed to Fight Smugglers". Sunday Star-Ledger, October 11, 1970.

_____, "Crime Fighting Computers". News Release of the Newhouse News Service, July 2, 1970. Washington, D.C.

Waldron, Martin, "Oklahoma Suit Challanges Secret Files on Activists". New York Times, October 30, 1970. New York.

Wall Street Journal, "Exchanges Ask Access to Fingerprint Data to Check Employees as Stock Thefts Rise". March 5, 1969. New York.

Westin, Alan F., "The Snooping Machine". Playboy, May, 1968

Zimmerman, Fred L., "Sale of Mailing Lists By Federal Agencies Irks Some in Congress". The Wall Street Journal, n.d., New York.

BIBLIOGRAPHY: ARMY CONUS INTELLIGENCE

"Army Maintains Deterrent Power over Civilian Rights", Senator S. J. Ervin, Congressional Record, July 29, 1970.

"Army on 24 Hour Alert for City Riots", The Washington Post, July 13, 1969.

"Army Riot Unit Marks Time", The Washington Post, Aug. 11,1968.

Congressional Record, March 2, 1970.

National Broadcasting Company, "First Tuesday", television broadcast, December 1, 1970.

Personal interview with Colonel John Downie, Director of Counterintelligence and Security in the Office of the Assistant Chief of Staff for Intelligence.

Personal interview with Mr. Ronald Greene, assistant to Army General Council Robert E. Jordan.

Personal interview with Herbert Holliman, formerly President of University of Oklahoma.

Personal interview with General Harold K. Johnson, U.S. Army, retired, formerly Chief of Staff of the Army.

Personal interview with Christopher H. Pyle, PhD candidate at Columbia University and former Captain of Army intelligence.

Pyle, Christopher H., "CONUS Intelligence: The Army Watches Civilian Politics", The Washington Monthly, January 1970.

_____., "CONUS Revisited: The Army Covers Up", The Washington Monthly, July 1970.

"The Spy who Went to Notre Dame", The Daily Cardinal, University of Wisconsin, May 20, 1970.

WGBH TV, "The Advocates", television broadcast, Boston, October 27, 1970.